

VŠB – Technická univerzita Ostrava

Fakulta elektrotechniky a informatiky

Katedra informatiky

Biometrické ověřování identity

Biometric Authentication

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Zadání diplomové práce

Student:

Bc. Marián Koniar

Studijní program:

N2647 Informační a komunikační technologie

Studijní obor:

2612T025 Informatika a výpočetní technika

Téma:

Biometrické ověřování identity
Biometric Authentication

Zásady pro vypracování:

Cílem práce je teoreticky rozebrat využití biometrie pro ověřování identity studentů při vykonávání testu v systému eLogika na základě otisku prstu a následný návrh a implementace.

V práci student:

1. Seznámí s teorií biometrického ověřování identity.
2. Seznámí s právními aspekty využívání biometrických údajů.
3. Navrhne, jakým způsobem ukládat a zabezpečit biometrické údaje v IS eLogika v souladu s právní normou.
4. Seznámí se stávajícím stavem (metody, jejich výhody, nevýhody, použití).
5. Analyzuje, navrhne a implementuje aspoň jednu metodu (předpokládá se zaměření na rozpoznání tváře či otisku prstů).
6. Proveďte analýzu a testování naimplementované metody. Předpokládá se chybovost do 10% na předložené rozpoznání.

Implementace bude využita v systému eLogika a bude programována v jazyce C#.

Seznam doporučené odborné literatury:

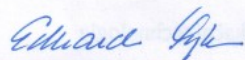
Podle pokynů vedoucího diplomové práce.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Mgr. Marek Menšík, Ph.D.**

Datum zadání: 18.11.2011

Datum odevzdání: 04.05.2012



doc. Dr. Ing. Eduard Sojka
vedoucí katedry



prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prehlásenie:

„Prehlasujem, že som túto diplomovú prácu vypracoval samostatne. Uviedol som všetky literárne
pramene a publikácie, z ktorých som čerpal.“

V Ostrave dňa 4.5.2012

A handwritten signature in blue ink, consisting of a series of loops and a long horizontal stroke, positioned above a dotted line.

podpis

Podakovanie

Chcel by som poďakovať hlavne vedúcemu mojej diplomovej práce Mgr. Marekovi Menšíkovi, Ph.D., že mi poskytoval cenné rady a pripomienky pri realizácii môjho projektu.

Abstrakt

Práca popisuje biometriu ako vednú disciplínu a charakterizuje jednotlivé biometrické metódy. Hlavná časť práce je venovaná odtlačkom prstov. Odtlačky prstov sú najstaršou biometrickou metódou. Algoritmy, pre identifikáciu a verifikáciu osôb sú už dlhodobo rozšírené v aplikáciách rôzneho charakteru. Kritickým bodom v ich ďalšom spracovaní je kvalita vstupného obrazu. V práci je popísaná metóda vylepšenie kvality obrazu Gaborovými filtrami. Jej obsahom je popis detekcie markantov a porovnávanie odtlačkov. V jazyku C# bola vytvorená aplikácie pre identifikáciu a verifikáciu osôb pomocou odtlačkov.

Kľúčové slová

Odtlaček prsta, markant, porovnávanie odtlačkov prstov, C#, snímač odtlačkov prstov, Gaborova filtrácia, vylepšenie obrazu, biometria

Abstract

This thesis describes biometrics as a scientific discipline and characterizes chosen biometric methods. Main part of the work is focused on fingerprints. Fingerprints are the oldest biometric method. Algorithms for identification and verification of individuals are expanded in applications of a various characters for a long time. Critical point for the next stages of processing is quality of input image. Fingerprint image enhancement method using Gabor filtering is described in Thesis. This work contains description of minutiae detection and fingerprint matching. An application for identification and verification of individuals using fingerprints was implemented in C#.

Keywords

Fingerprint, minutiae, fingerprint matching, C#, fingerprint reader, image enhacment, Gabor filtering, biometrics

Obsah

1	Úvod	2
1.1	Obsah práce	2
2	Základné pojmy v biometrii	3
2.1	Biometrický systém	3
2.2	Prehľad biometrických identifikačných metód používaných v praxi	5
2.3	Výkonnosť biometrických systémov	10
3	Odtlačok prsta	15
4	Spôsoby získania odtlačkov prstov	21
5	Predspracovanie obrazu odtlačku	27
5.1	Gaborova filtrácia	28
6	Analýza odtlačku	37
6.1	Hľadanie a označenie markantov	37
7	Porovnávanie odtlačkov prstov	41
8	Právna problematika využitia biometrických údajov	44
9	Implementácia v systéme eLogika	48

1 Úvod

Práca popisuje najpoužívanejšie biometrické metódy v praxi. Hlavná časť práce je venovaná odtlačkom prstov a ich jedinečnosti. Charakterizuje jednotlivé typy snímačov odtlačkov prstov, ich výhody a nevýhody. Zaoberá sa predspracovaním obrazu metódou Gaborových filtrov, detekciou markantov, porovnávaním odtlačkov prstov a popisuje s tým súvisiacu právnu problematiku.

Cieľom práce je teoreticky popísané postupy implementovať a vytvoriť aplikáciu pre správu odtlačkov prstov, ktorá umožní verifikáciu a identifikáciu študentov. Ďalším krokom je vytvorenie aplikácie, ktorá umožní študentovi absolvovať skúšku v prostredí systému eLogika po overení identity odtlačkom prsta.

1.1 Obsah práce

Text práce je usporiadaný do jednotlivých kapitol.

Kapitola Základné pojmy v biometrii popisuje biometriu ako vednú disciplínu, sú v nej popísané základne pojmy, nutné pre pochopenie popisovanej problematiky v ďalších častiach práce. Táto kapitola ponúka náhľad na najpoužívanejšie biometrické metódy v praxi.

V kapitole Odtlačky prstov je popísaná ich historická cesta k dnešnej najpoužívanejšej biometrickej vlastnosti. Popisuje význam papilárnych línií, ich vlastnosti a usporiadanie, ktoré ich robia jedinečnými.

Spôsoby získania odtlačkov prstov je kapitola, v ktorej sú popísané spôsoby získavania odtlačkov prstov pre ďalšie elektronické spracovanie. Kapitola popisuje rôzne snímače odtlačkov prstov.

Kapitoly Predspracovanie obrazu odtlačku, Analýza odtlačku a Porovnávanie odtlačkov prstov popisujú cestu odtlačku prsta od jeho získania cez úpravy obrazu, extrakciu charakteristických znakov až po získanie biometrickej šablóny a ich porovnávanie.

Kapitola Právna problematika využitia biometrických údajov rozoberá právne predpisy a normy súvisiace so spracovaním biometrických a osobných údajov

Kapitola Implementácia v systéme eLogika popisuje implementáciu a realizáciu aplikácii pre spracovania rozpoznávania odtlačkov prstov.

2 Základné pojmy v biometrii

V tejto kapitole som vychádzal z týchto zdrojov [1], [2], [3], [4], [5].

Biometria (biometric) je vedná disciplína, ktorá sa zaoberá štúdiom živých organizmov (bio-), predovšetkým človeka a meraním (-metric) jeho biologických vlastností, ale aj jeho správaním (behaviorálne charakteristiky). V prenesenom význame sa však jedná o meranie a rozpoznávanie určitých charakteristík človeka. Biometria sa venuje štúdiu metód, ktoré vedú k rozpoznávaniu človeka na základe jeho unikátnych proporcií alebo vlastností. Rozpoznávanie ľudí na základe biologických charakteristík bolo využívané už v dávnej minulosti, ľudia sa rozpoznávajú podľa vzhľadu tváre. Sú známe odtlačky dlaní v jaskyniach pri maľbách ako istá forma podpisu autora, pričom niektoré z nich sú 30000 rokov staré. S rozvojom počítačových technológií koncom šesťdesiatych rokov dvadsiateho storočia sa biometrické rozpoznávanie človeka začalo automatizovať. V tejto problematike je dôležité porozumieť základným pojmom.[2]

Recognition (rozpoznávanie) - je druhový termín, ktorý nutne nemusí znamenať identifikáciu ani verifikáciu. Jedná sa o rozpoznávanie človeka pri použití vhodnej telesnej vlastnosti.

Verification (overenie, verifikácia) - proces, pri ktorom sa biometrický systém pokúša potvrdiť totožnosť jedinca, porovnaním odobratej vzorky s už predtým zapísaným záznamom tzv. šablónou (template). Princíp známy taktiež pod pojmom one-to-one (1:1).

Identification (identifikácia) - je proces, kedy sa biometrický systém snaží určiť totožnosť neznámeho jedinca. Biometrická informácia je získaná a porovnávaná so všetkými uloženými šablónami. Princíp známy taktiež pod pojmom one-to-many (1:N).

Authentization (autentizácia, autentifikácia alebo legalizácia) - termín môžeme zlúčiť s pojmom rozpoznávanie. Avšak na konci tohto procesu získa užívateľ určitý status.

2.1 Biometrický systém

Biometrický systém je v podstate systém rozpoznávajúci fyziologické a behaviorálne charakteristiky. Hlavnou otázkou pri navrhovaní biometrického systému je spôsob ako rozpoznávať jedinca. V závislosti od kontextu aplikácie sú rozlišované overovacie a identifikačné systémy.

Verification system

Systém overí totožnosť osoby na základe porovnania biometrickej charakteristiky s biometrickou šablónou vopred uloženou v systéme. Systém na základe porovnávania overí, či je osoba skutočne tou osobou za ktorú sa vydáva. Systém buď prijme alebo odmietne predloženú žiadosť (princíp „Som kto tvrdím, že som?“). Keďže sa jedná o porovnávanie zvyčajne dvoch biometrických šablón, je verifikačný proces rýchlejší ako identifikácia. Verifikačný proces je využívaný hlavne v komerčnej sfére.

Identification system

Identifikačný systém porovnáva jedinca s kompletnou databázou biometrických šablón. Porovnávaním 1:N sa snaží zistiť jeho totožnosť. Identifikačný systém zistí totožnosť jedinca, bez toho aby ju uviedol. (princíp „Kto som?“) Tento proces môže byť v závislosti na veľkosti databáze výpočtovo veľmi náročný. Identifikačný proces je najčastejšie používaný v kriminalistike.

Využitie elektronických biometrických systémov má v praxi široké uplatnenie, nech už sa jedná o súkromnú, štátnu alebo forenznú sféru. Vo forenznej (súdna, kriminalistická ,vyšetrovacía) sfére je najznámejší a najviac používaný systém AFIS (Automated Fingerprint Identification System - Automatizovaný systém pre identifikáciu podľa odtlačku prstu). Systém AFIS bol vyvinutý vládou USA v spolupráci s FBI (Federal Bureau of Investigation - Národný vyšetrovací úrad) a v spolupráci s NIST (National Institute of Standards and Technology). Hlavný rozdiel u súkromného systému je v omnoho menšej databáze biometrických vzorkov a samotných osôb. Taktiež nie je nutné ukladať a získavať odtlačky všetkých prstov ako je to bežné v kriminalistike. Takýto systém si vystačí s omnoho menšou kapacitou pamäte a hlavne operačným výkonom.

Predpokladom pre prevedenie biometrickej autentifikácie je získanie a zápis biometrickej informácie osoby, ktorá je ďalej spracovaná a uložená ako šablóna.

Väčšina biometrických systémov pracuje týmto spôsobom:

- Získanie dátového súboru (obraz, zvuk, atd.), ktorý obsahuje biometrickú vlastnosť, ktorú je možné extrahovať použitím vhodného snímača.
- Preverenie kvality dát: pokiaľ kvalita týchto dát nie je dostatočná, sú okamžite odmietnuté alebo je užívateľovi poskytnutá vhodná rada pre zvýšenie kvality biometrickej vlastnosti (upozornenie na zmenu spôsobu priloženia prsta).
- Vyextrahovanie požadovanej biometrickej veličiny z dátového súboru a vytvorenie biometrickej šablóny (template).

- Zápis: vyextrahovaná šablóna je uložená ako referenčná šablóna do archívu referenčných šablón systému alebo aplikácie (podľa definovaného úložiska).
- Overenie: porovnanie aktuálnej šablóny s referenčnou šablónou použitím algoritmu pre určenie zhody a výpočet miery podobnosti (skóre).
- Výsledok overovania: Žiadosť je prijatá pokiaľ miera podobnosti prekročí medznú hranicu (threshold) v opačnom prípade je žiadosť odmietnutá.

Kritéria pre výber biologickej alebo behaviorálnej charakteristiky človeka pre jeho identifikáciu sú determinované čo najširším a najefektívnejším spôsobom použitia. Takáto charakteristika musí spĺňať:

- **Jednoznačnosť:** vlastnosť musí byť čo najviac výnimočná, čiže rovnaká hodnota vlastnosti sa nesmie vyskytnúť u dvoch rôznych jedincov.
- **Univerzálnosť:** vlastnosť musí byť merateľná u čo najväčšej množiny ľudí.
- **Trvalosť:** vlastnosť musí byť v čase nemenná.
- **Merateľnosť:** vlastnosť musí byť merateľná technickým zariadením.
- **Užívateľská prijateľnosť:** vlastnosť musí byť pohodlne merateľná.

2.2 Prehľad biometrických identifikačných metód používaných v praxi

Odtlačky prstov – Fingerprints

Odtlačky prstov tvoria akýsi symbol biometrickej identifikácie. Sú využívané viac ako 100 rokov a rovnakú dobu sú aj súdne akceptovateľné. Odtlačky prstov sú uznávané ako celosvetový štandard policajno-súdnej, bezpečnostnej a komerčnej identifikácie. Táto metóda vychádza z unikátnosti obrazov papilárnych línií.

Očná dúhovka – Iris

Farebný kruh, ktorý sa nachádza okolo zornice ľudského oka obsahuje špecifické a unikátne identifikačné body. Pomocou týchto bodov je možné s veľkou presnosťou stanoviť identitu osoby. Dúhovka sa skladá z náhodne rozmiestnených a v čase nemenných farebných štruktúr. Žiadne dve dúhovky oka nie sú rovnaké. Snímanie prebieha pomocou štandardnej video technológie.

Očná sietnica – Retina

Obsahuje rovnako dostatok špecifických anatomických bodov, ktoré zaisťujú vysokú identifikačnú presnosť. Zosnímanie biometrickej vzorky prebieha svetelným lúčom. Biela sietnica ľudského oka časť lúča pohltí a časť absorbuje. Takto je zmapované riečisko žíl a cievok sietnice, ktoré zostáva počas života takmer nemenne.

Geometria ruky –Hand Geometry

Je najstaršia plne automatizovaná bezpečnostne - komerčná identifikácia osoby, realizovaná na základe anatomicko - geometrických charakteristík ľudskej dlane a prstov. Podstatou tejto metódy je dvoj alebo trojrozmerné meranie dĺžok alebo širok jednotlivých prstov, kĺbov alebo kostí. Metóda bola po prvý krát použitá na ochranu prístupu k burzovým informáciám a v objektoch amerického jadrového výskumu.

Hlas – Voice

Ľudský hlas taktiež obsahuje určité biometrické charakteristiky, ktoré sú nezameniteľné. Ľudský hlas ma fyziologické ale aj behaviorálne charakteristiky. Akustický signál hlasu je transformovaný za normálnych okolností do unikátneho digitálneho kódu.

Tvár – Face

Tvár je taktiež vlastná a špecifická pre každú osobu. Počítačové technológie dokážu rozpoznávať tváre jednotlivých ľudí podobným spôsobom ako človek. Ľudská tvár obsahuje identifikačné (antropologické) body, ktoré sú špecifické a v čase nemenné.

Podpis –Signature

Dnes sa už nerozoznáva len statický obraz podpisu, ale aj dynamické charakteristiky ako je jeho písanie, rýchlosť, tlak pri písaní, smer podpisu a ďalšie relačné charakteristiky.

DNA

Reťazec DNA má všetky predpoklady na to aby sa stal najpresnejším a najspoľahlivejším identifikátorom ľudskej osobnosti. Obsahuje obrovské množstvo informácií o každej osobe a len nepatrná časť týchto informácií je potrebná a dostačujúca pre identifikáciu osoby. Po analógii s daktyloskopickým odtlačkom sa o DNA ako biometrickej charakteristike používa termín genetický odtlačok.

Biometrická metóda	Snímanie	Nemennosť	Jednoznačnosť	Prijateľnosť
Geometria ruky	Optické-infračervené	Dobrá	1:10 000	Veľmi dobrá
Očná sieťnica	Optické-laser	Veľmi dobrá	1:1 000 000	Nedobrá
Očná dúhovka	Optické	Veľmi dobrá	1:6 000 000	Nedobrá

Štruktúra žíl na zápästí	Optické-infračervené	Dobrá	Neznáma	Veľmi dobrá
Podpis	Statický obraz alebo dynamické snímanie	Premenlivá	1:10 000	Veľmi dobrá
Hlas	Elektroakustické	Premenlivá	1:10 000	Dobrá
Tvár	Optické, infračervené	Dobrá	Neznáma	Dobrá
Odtlačok prsta	Optické, kapacitné ..	Veľmi dobrá	1:1 000 000	Dobrá

V nasledujúcich kapitolách uvádzam stručný popis niektorých biometrických metód. Spracovaniu a rozpoznávaniu odtlačkov prstov sa venuje kapitola Odtlačok prsta.

Dynamika podpisu

Táto metóda využíva jedinečnosť kombinácie anatomických a behaviorálnych charakteristík človeka, ktoré sa prejavujú až keď sa človek podpisuje. Zariadenie pre dynamický podpis je často zamieňané s pojmom elektronický podpis (šifrovaný kľúč) alebo so zariadeniami určenými pre snímanie podpisu ako obrazu. Z ručného podpisu je takto možné určiť ťah, tvar a tlak pri písaní, čo je uplatniteľné pri verifikácii osoby. Väčšina týchto zariadení využíva dynamické vlastnosti podpisu, ale existujú aj zariadenia, ktoré kombinujú statické a dynamické vlastnosti podpisu. Základnými dynamickými vlastnosťami sú rýchlosť, akcelerácia, časovanie, tlak a smer ťahu, ktoré sú zaznamenané v trojrozmernom súradnicovom systéme. Osy x a y určujú rýchlosť a smer ťahu, súradnica z určuje tlak na podložku. Jeho výhodou je, že na rozdiel od statického podpisu, ktorý je ľahko napodobiteľný je dynamiku podpisu takmer nemožné naučiť sa. Táto metóda však umožňuje len verifikačný princíp.

Geometria tváre

Identifikácia osôb založená na rozpoznávaní tváre je stará ako ľudstvo samé. Dnes je to najviac skúmaná metóda, pretože problematika identifikácie osôb podľa ich tváre je veľmi obsiahla.

Identifikácia osoby na základe jej tváre má v porovnaní s metódou odtlačkov prstov alebo očnej dúhovky nižšiu identifikačnú jednoznačnosť. Metóda umožňuje bezkontaktné snímanie a je pre užívateľa akceptovateľná pre svoju prirodzenosť na rozdiel od iných biometrických metód. Identifikácia osoby podľa jej tváre má dve kľúčové etapy. V prvej prebieha detekcia a lokalizácia tváre, čiže jej priestorové umiestnenie. V druhej etape prebieha automatické nájdenie základných identifikačných charakteristík a samotná identifikácia, teda rozpoznanie tváre medzi tvármi ktoré systém už pozná.

Detekcia a lokalizácia tváre závisí na typu scény. Je pomerne jednoduché detekovať a rozpoznať tvár napríklad v aplikáciách ako je prihlasovanie sa do počítača, kde je štandardné pozadie a vzdialenosť od snímacej kamery je vo vymedzenom rozsahu. V aplikáciách reálneho charakteru je táto situácia podstatne zložitejšia. Na scéne sa pohybuje veľké množstvo iných osôb. Ich detekcia a lokalizácia je náročná, pretože vzdialenosť od snímacej kamery nemá pevne určený rozsah a niektoré identifikačné znaky tak nie je možné odlíšiť.

Z hľadiska použitia výpočtových algoritmov pri spracovaní obrazu tváre rozlišujeme počítačové technológie založené na znalostných pravidlách, pravidlách štatistického rozhodovania, neurónových sieťach, genetických algoritmov a mnoho ďalších.

Dúhovka oka

Biometrické systémy pre rozpoznávanie dúhovky oka sú pomerne nové. Prvý patent pochádza z roku 1994. Dúhovka je farebná časť oka a jej zafarbenie odpovedá množstvu melatoninového pigmentu. Aj keď je zafarbenie a štruktúra dúhovky genetiky závislá, jej vzorkovanie nie. Dúhovka sa vyvíja behom prenatálneho štádia a jej vzorkovanie je náhodné, teda rozdielna pre každého človeka i jednovaječné dvojčatá. Dokonca aj jeden človek má každú dúhovku inú, čo činí tieto systémy najpresnejšie zo všetkých.

K snímaniu dúhovky je využívané infračervené osvetlenie oka. Behom snímania sa dúhovka mapuje do diagramov, ktoré obsahujú informáciu o orientácii, početnosti a pozícii špecifických plôch. Pomocou týchto informácií je vytvorená dúhovková mapa a šablóna pre identifikáciu. Pri verifikačnom procese sa porovnáva žiadateľova mapa dúhovky s referenčnou pomocou testu štatistickej nezávislosti. V prípade ak je len menej ako jedna tretina dát odlišná, test štatistickej nezávislosti zlyhal, čo znamená že vzorky sú z rovnakej dúhovky.

Sietnica oka

Pre rozpoznanie osoby podľa sietnice sa používa obraz štruktúry ciev na pozadí ľudského oka v okolí slepej škvrny. Sietnica je na svetlo citlivý povrch na zadnej strane oka a je tvorená veľkým množstvom nervových buniek. Obraz sa získava pomocou zdroja svetla s nízkou intenzitou žiarenia a optoelektronického systému. Naskenovaný obraz je prevedený do podoby 40 bitového čísla. Je to veľmi presná metóda spôsobu identifikácie, vyžaduje však od užívateľa, aby sa pozeral do presne vymedzeného priestoru, čo môže byť však v niektorých prípadoch nepríjemné alebo nemožné. Z tohto dôvodu nemá táto metóda rozšírenú oblasť používania a jej použitie je len v oblastiach najvyššieho stupňa zabezpečenia.

Geometria ruky

- kombinácia dĺžky, šírky a hrúbky ruky, meranej na všetkých piatich prstoch jednej ruky, ich tvar (obrys, kontúra) sú jedinečné a je na nich možné založiť veľmi presnú verifikáciu osôb. Zariadenie sníma ruku položenú na podložke s piatimi polohovými kolíkmi. Systém rozpoznávajúci geometriu ruky je najstarším implementovaným biometrickým systémom. Sú používané v dochádzkových a prístupových systémoch, kde sú pomerne rozšírené. Väčšina amerických atómových elektrární používa metódu geometrie ruky pre reguláciu vstupu osôb. Tieto skenery sú používané v pilotných projektoch hraničnej kontroly alebo v bankovníctve.

Výhody: Metóda je pre užívateľa veľmi jednoduchá a rýchla. Užívateľ sa behom niekoľko málo pokusov naučí správne prikladať ruku k snímacej ploche. Nezávislé testovania v laboratóriách Sandia potvrdili, že metóda je pre užívateľov prijateľnejšia ako biometrické metódy založené na vyhodnocovaní odtlačkov prstov, hlasu alebo sietnice oka.

Nevýhody: Metóda je použiteľná len pre verifikáciu, ale nie pre identifikáciu, pretože z biometrickej šablóny nie je možné jednoznačne spätne identifikovať osobu, ktorá jej patrí. Tento nedostatok je z určitého pohľadu výhodou. Nedochádza k pocitu narušovania osobných údajov a tak metóda poskytuje kontrolovaným osobám dostatok súkromia.

Štruktúra žíl na zápästí

Je jednou z najnovších metód rozpoznávania osôb. Prvý komerčne dostupný systém pochádza z roku 2000. Veľkou výhodou tejto metódy je, že štruktúra žíl je ťažko falšovateľná (sieť ciev na zápästí je ťažké napodobniť. Niektoré systémy priamo overujú živosť snímanej ruky). Technológia spočíva v snímaní kamerou v infračervenom svetle. Štruktúra krvného riečiska sa u dospelého človeka príliš nemení, je veľmi výrazná a odlišná pre pravú a ľavú ruku a jej jedinečnosť je preukázaná aj u jednovaječných dvojčiat. Metóda poskytuje možnosť verifikácie aj identifikácie.

Použitím zobrazenia v spektre, ktoré je blízke infračervenému svetlu sa zvýrazní kontrast medzi cievnyim riečiskom a okolitou kožou. Ďalšie spracovanie je podobné ako pri spracovaní odtlačkov prstov. Pomocou vybraných algoritmov sa prevádzajú rôzne konverzie pre potlačenie šumu, a vytvorenie kostry obrazu a nakoniec vytvorenie binárnej biometrickej šablóny.

Metóda má rovnaké využitie ako metóda geometrie ruky. K tomu má lepšie možnosti pre miniaturizáciu takže sa predpokladá jej využitie u bankomatov, automobilových dverových zámkov. Metóda bola použitá na britských univerzitách na kontrolu identity študentov skladajúcich skúšku.

Hlas

Kriminalistika využíva porovnávanie vzoriek hlasu už desiatky rokov. V civilnej praxi sa táto technológia presadzuje až v posledných rokoch. Na overovanie identity slúži uložená vzorka hlasu,

ktorá je tvorená nahovorenou kľúčovou vetou. Výhoda overenia identity pomocou hlasu spočíva nielen v špecifickosti ľudského hlasu ale aj vo flexibilitě kľúčových viet. Identifikácia pomocou hlasu, teda rozpoznanie hlasu medzi inými v reálnom prostredí je o mnoho náročnejšia a v súčasnosti neexistuje dostatočne presný systém. Hlavnou výhodou verifikácie identity pomocou digitálnych odtlačkov hlasu je nízka cena, pomerne veľká spoľahlivosť a široká možnosť nasadenia od telefónneho bankovníctva až po vzdialený prístup k informačným systémom.

DNA

DNA je ako identifikačný prvok používaný v policajnej praxi od druhej polovice osemdesiatych rokov. Štruktúra DNA je odlišná u všetkých ľudí s výnimkou jednovaječných dvojčiat. Presnosť skúmania DNA je dôvodom pre stále širšie využitie tejto technológie i keď získanie odtlačku DNA predstavuje pomerne náročnou a zdĺhavú procedúrou, ktorá sa skladá z týchto krokov. Zo vzorky tkaniva je vypreparovaná celá špirála DNA, ktorá je následne štepená enzýmom EcoR1 a následné sú fragmenty DNA vylučované až sa získa reťazec využiteľnej veľkosti. Získané fragmenty sú prenesené na nylónovú membránu a po pridaní rádioaktívnych alebo zafarbených génových sond je získaný röntgenový snímok - odtlačok DNA. Tento odtlačok pripomína čiarový kód a preto je jednoduché ho previesť do elektronickej podoby. Takto získaná informácia slúži na riešenia celej rady otázok. Pre problémy, ktoré potrebujú svoje riešenie v reálnom čase je však táto technológia zatiaľ nepoužiteľná.

2.3 Výkonnosť biometrických systémov

Existuje veľká rada charakteristík, ktorými môžeme porovnávať rôzne biometrické metódy. Efektívnosť biometrických systémov je možné merať množstvom štatistických koeficientov. Rozhodujúcimi kritériami pri výbere zariadenia môže byť rýchlosť spracovania samotného porovnávania, kapacitné možnosti (počet identifikácií a verifikácií v určitej časovej jednotke), užívateľská prijateľnosť, cena, spoľahlivosť, odolnosť apod. Toto ale nie sú tie najdôležitejšie kritéria.

Identifikácia a verifikácia osoby má vždy bezpečnostný charakter. Cieľom je, aby oprávnená osoba mala vždy pridelené garantované práva (prístup do systému apod.) naopak osoba, ktorá tieto práva nemá, musí byť odmietnutá. V krajnom prípade môže byť táto osoba podvodník. Podobná situácia je v kriminalistickej sfére, kde je vyžadované bezchybné stotožnenie osoby, ktorá sa už v minulosti podieľala na trestnej činnosti a zároveň je nežiaduca zámena totožnosti s inou osobou. Preto boli v praxi zavedené tieto dva základne pojmy pracujúce s pravdepodobnosťou oboch nežiaducich javov.

Pravdepodobnosť chybného prijatia (neoprávnenej osoby)

False Acceptance Rate (FAR). V anglickej literatúre je FAR niekedy nahrádzaný za pojem False Match Rate (FMR).

Pravdepodobnosť chybného odmietnutia (autorizovanej osoby)

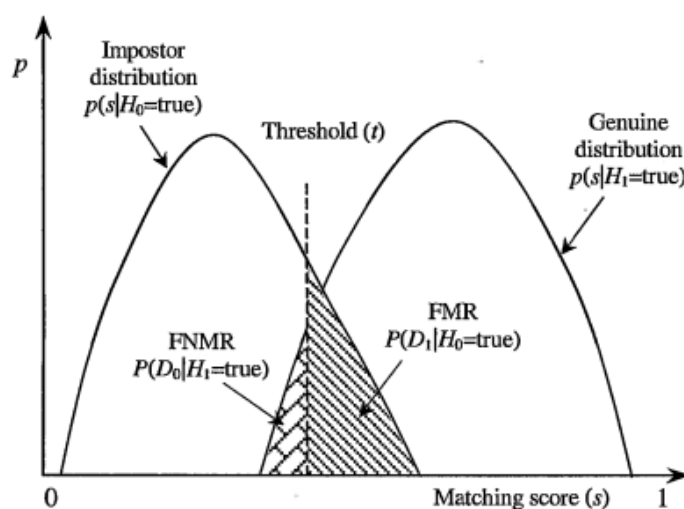
False Rejection Rate (FRR). V anglickej literatúre je niekedy FRR nahrádzaná za ekvivalentný pojem False Non Match Rate(FNMR).

Pravdepodobnosť chybného prijatia alebo odmietnutia biometrických metód nie je možné teoreticky vypočítať. Biometrické metódy identifikácie a verifikácie sú založené na štatistickom vyhodnocovaní podobnosti zosnímanej biometrickej informácie a uloženej šablóny. Pri snímaní biologického vzoru nie sú zaznamenané rovnaké hodnoty. V dôsledku toho sa obe porovnávané šablóny vždy líšia. Výsledkom procesu porovnávania je miera totožnosti (skóre), ktorá je zakaždým iná. Platí, že čím nižšie FAR tým je vyššie FRR a naopak. Hodnota pri ktorej je FAR a FRR rovnaká sa nazýva ERR(Equal Error Rate).

Biometrická šablóna P' a na snímajúcom zariadení je nabitý biometrický vzorok P . mieru totožnosti (skóre s) vypočítame ako:

$$s = \text{Sim}(P, P').$$

Aplikácia má prah citlivosti Th , platí, že ak je $s \geq Th$, potom $P = P'$ a majiteľ vzorku P je vyhodnotený ako oprávnená osoba (stav H_0). Ak $s < Th$ tak $P \neq P'$, majiteľ vzorku P je vyhodnotený ako osoba neoprávnená, pretože nebola nájdená požadovaná miera podobnosti (Obrázok 2.1).



Obrázok 2.1 histogram stotožnenia oprávnených a neoprávnených osob[1]

False Rejection Rate

Koeficient FRR udáva pravdepodobnosť toho, že oprávnený užívateľ je systémom odmietnutý. Tento koeficient udáva komfort, pretože nesprávne odmietnutie je pre užívateľa nepríjemné. Označuje sa ako chyba I. druhu (Type I Error Rate). Je to odmietnutie osoby, ktorá je v systéme registrovaná, má mať za normálnych podmienok oprávnený prístup. U civilných aplikácií sa nejedná o kriticky negatívny

jav, núti však užívateľa k opakovanému pokusu o prístup a ma za následok jeho nespokojnosť. Je samozrejmé, že v praxi nie je žiaduce aby systém odmietal veľký počet oprávnených osôb, pretože klesá dôvera v daný systém. V kriminalistike však falošné odmietnutie znamená, že osoba u ktorej ma dôjsť k potvrdeniu identity nie je rozpoznaná a tak nie je potvrdená ani jej identita. Osoba touto chybou môže uniknúť z vyšetrovania a to je považované za závažnú chybu a nedostatok.

Pravdepodobnosť chybného odmietnutia (FRR) je definovaná ako:

$$FRR = \frac{N_{FR}}{N_{EIA}} \text{ alebo } FRR = \frac{N_{FR}}{N_{EVA}},$$

kde :

N_{FR} - Number of False Rejection (počet chybných odmietnutí),

N_{EIA} - Number of Enrolle identification Attempts (počet oprávnených osôb o identifikáciu),

N_{EVA} - Number of Enrolle Verification Attempts (počet oprávnených osôb o verifikáciu).

False Acceptance Rate

Pravdepodobnosť toho že neoprávnený užívateľ je prijatý systémom ako oprávnený. FAR je koeficient, ktorý určuje mieru bezpečnosti systému. Označuje sa ako chyba II. Druhu (Type II Error Rate) . Ide o prijatie, pripustenie neregistrovanej osoby do systému. Táto osoba nemá za normálnych podmienok oprávnený prístup. Z bezpečnostného hľadiska sa jedna o závažnú chybu. V aplikáciách a systémoch kontrolujúcich určitú formu prístupu, je chybné prijatie neoprávnenej osoby nutne chápať ako bezpečnostný incident dôsledkom ktorého môže dôjsť k nežiaducim aktivitám. V kriminalistike falošné prijatie znamená, že osobe je pridelená cudzia identita. V praxi môže byť teda osoba identifikovaná chybne a vyšetrovanie môže pokračovať zlým smerom.

Pravdepodobnosť chybného prijatia FAR je definovaná ako :

$$FRR = \frac{N_{FA}}{N_{IIA}} \text{ alebo } FAR = \frac{N_{FA}}{N_{IVA}},$$

kde:

N_{FA} - Number of False Rejection (počet chybných odmietnutí)

N_{IIA} - Number of Impostor Identification Attempts (počet neoprávnených osôb o identifikáciu)

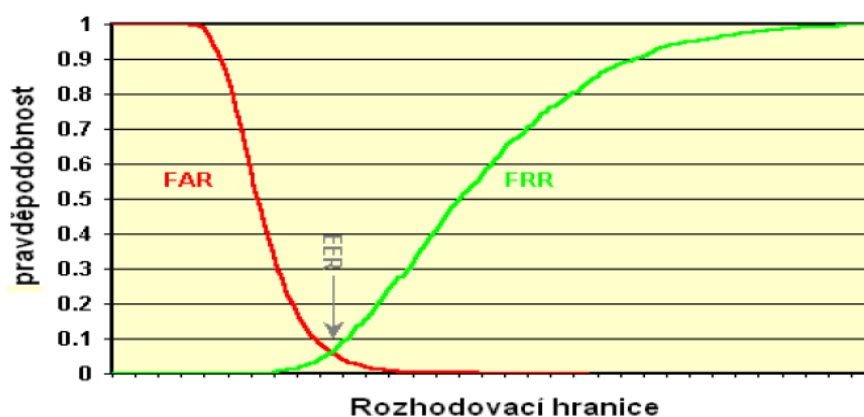
N_{IVA} - Number of Impostor Verification Attempts
(počet pokusov neoprávnených osôb o verifikáciu)

Vzťah medzi FRR A FAR

Ideálna aplikácia nevykazuje žiadnu chybovosť ani nespoľahlivosť. Všetky preverované osoby sú stopercentne rozpoznané, čiže neexistujú ani neoprávnené prijaté osoby a ani neoprávnene odmietnuté osoby. V tomto prípade všeobecne platí že,

$$FAR = FRR = 0$$

Takáto aplikácia alebo zariadenia však neexistuje, pretože každé reálne zariadenie je rôzne citlivé na vonkajšie vplyvy ovplyvňujúce jeho činnosť(Obrázok 2.2). znázorňuje prienik FAR a FRR. Je zrejmé, že biometrický systém môže mať v určitom čase jediné pevné nastavenie prahu(threshold). Podľa jeho nastavenia sa bude odvíjať chovanie biometrického systému. V prostredí, kde je požadovaná vysoká bezpečnosť sa musíme zmieriť s tým, že niektoré oprávnené osoby budú považované za neoprávnené. Ak však budú kladené požiadavky na pohodlie užívateľov, musíme sa zmieriť s tým, že systém bude „deravý“ a teda môže prepustiť do systému aj neoprávnené osoby.



Obrázok 2.2 Vzťah medzi FRR A FAR [2]

Ďalšie výpočty chybovosti

V niektorých prípadoch je lepšie mať detailnejší prehľad o dôvodoch chybovosti zariadenia. Preto je možné chybovosti FAR a FRR jemnejšie rozdeliť. Príkladom môže byť skupina ľudí, ktorí sa nemôžu zaregistrovať do systému, pretože majú chýbajúce články prstov(pri systéme založenom na odtlačkoch prstov). Užívateľ nebude môcť byť registrovaný do systému ,takýto situácia sa nazýva **Failure to Enroll** (FTE). Môže nastať situácia, keď je užívateľ registrovaný v systéme a získané biometrické dáta nie sú dostatočne kvalitné (počet extrahovaných markantov u odtlačku prstu). V tomto prípade je nutné opäť získať tieto dáta. Táto situácia sa nazýva **Failure to Acquire** (FTA). V prípade ak sú vstupné dáta v dostatočnej kvalite môžu sa porovnávať s uloženou šablónou (popríklad šablónami pri identifikačnom procese). Pri porovnávaní môže nastať situácia nesprávneho pridelenia cudzej

identity, teda nesprávne stotožnenie, anglicky **False Match** (FM), v prípade keď dôjde k nesprávnemu nestotožneniu jedna sa o **False Non Match** (FNM).

3 Odtlačok prsta

V tejto kapitole som vychádzal z týchto zdrojov [1], [2], [3], [4], [5], [10], [11], [12].

Identifikácia pomocou odtlačku prsta je jednou z najznámejších biometrických metód. Je používaná hlavne pre svoju jedinečnosť a nemennosť v čase a pre vysoké percento použiteľnej populácie.

3.1 História

Odtlačky prstov boli nájdené na množstve archeologických artefaktov a historických predmetoch. Aj keď tieto nálezy poskytujú dôkaz, že ľudia si boli vedomí jedinečnosťou odtlačkov, nezdá sa, že by mali vedecký základ. V roku 1684 Nehemiah Grew publikoval prvú vedeckú prácu v ktorej skúmal štruktúru odtlačkov prstov. V roku 1809 Thomas Bewick začal používať svoj odtlačok prstu ako obchodnú značku. Ján Evangelista Purkyně v roku 1823 vytvoril prvú klasifikáciu odtlačkov prstov, v ktorej delil odtlačky do deviatich kategórií na základe usporiadania papilárnych línií. Henry Fauld v roku 1880 prvý krát vyslovil myšlienku, že odtlačok každej osoby je jedinečný.

Počiatok modernej biometrie sa datuje od roku 1882, keď antropológ a vedúca osobnosť identifikácie páchatel'ov parížskej polície Alphonse Bertillion hľadal spôsob ako identifikovať už v minulosti odsúdených zločincov. Jeho zásluhou sa biometria stala reálnym predmetom štúdia. Bertillion vynášiel metódu, merania určitých fyzických charakteristík človeka, ktorá bola po ňom nazvaná Bertillonáž. Po čase však bolo zistené, že niektorí ľudia môžu mať tieto miery zhodné, preto sa systém Alphonsa Bertilliona sa prestal používať.

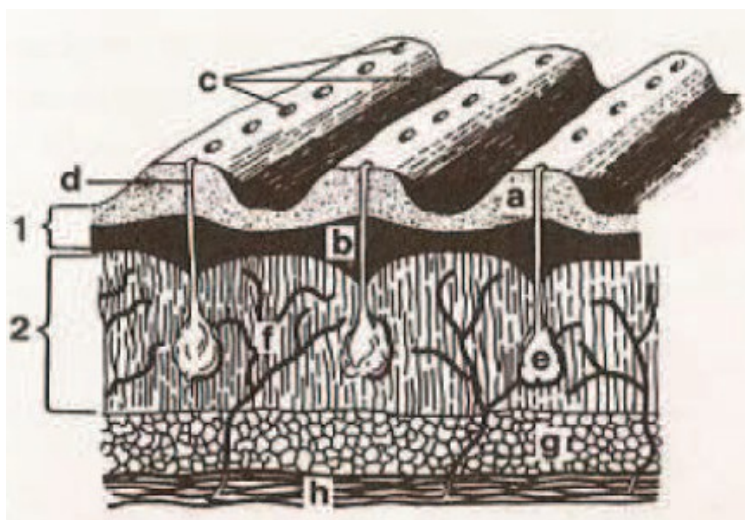
Joseph T. James publikoval v roku 1866 článok v ktorom vyvodil 2 hypotézy na ktorých dodnes stojí využitie odtlačkov prstov pre identifikáciu. V prvej hypotéze predpokladal, že papilárne línie na koncoch článkov prstov sú počas života nemenné. Druhá hypotéza predpokladala, že žiadny dvaja ľudia nemajú zhodné obrazce papilárnych línií.

Sir Francis Galton publikoval v roku 1888 pracú v ktorej definoval charakteristické body, ktoré slúžia k identifikácii človeka. Položil základy daktyloskopie. Galtonove body sa v súčasnosti označujú ako markanty (minutuae). Galton vypočítal, že existuje celkom 64 miliárd rôznych variant usporiadania papilárnych línií. Prakticky vylúčil že existujú dvaja rovnaký jedinci s totožným odtlačkom. Značný pokrok zaznamenal v roku 1899 Edward Henry, ktorý vytvoril nový klasifikačný systém (Henryho systém). Prvý krát prakticky využil odtlačky William James Herschel, ktorý takto overoval vyplácanie vojenskej penzie. Vylúčil tak možnosť podvodu a získal množstvo materiálu pre ďalší výskum.

3.2 Papilárne línie

Papilárne línie sa nachádzajú na dlaniach, prstoch ale aj na spodnej strane chodidiel. Na iných miestach ľudského tela sa papilárne línie nevyskytujú. Presný účel obrazcov tvorených týmito papilárnymi líniami nie je známy ale vieme, že ich význam je spojený s citlivosťou pokožky a hmatom[4].

Papilárne línie tvoria na povrchu dlane, dlaňovej strany prstov a chodidiel vyvýšené časti pokožky dosahujúce výšky 0,1 - 0,4 mm a šírky 0,2-0,7 mm (Obrázok 3.1). Tieto zvýšené časti pokožky vytvárajú obrazce, ktoré sú základom pre daktyloskopickú identifikáciu osôb. Koža ma dve základne vrstvy, vrchnú pokožku (*epidermis*), ktorá prichádza do kontaktu s vonkajším prostredím. Pod ňou je väzivová koža (*cutis* alebo *corium*). Medzi *epidermis* a spodnou väzivovou vrstvou (*Stratum papillae*, *corium*) sa nachádza vrstva *Stratum Malpighii*. Papily tvoria zložité obrazce, sú tým vyššie, čím väčšiu a jemnejšiu pohyblivosť vyžaduje určité miesto kože.



Obrázok 3.1 Stavba kože s papilárnymi líniami [4]

1 – pokožka (*epidermis*), 2 – škára (*curie*); a – rohová vrstva; b – zárodočná vrstva; c – póry; d – vývody potných žliaz; e – potné žľazy; f – cievy; g – podkožný tuk; h – svalstvo.

Z pohľadu kriminalistiky je veľmi dôležité aj to, že papilárne línie s výnimkou niektorých ľudopopov (podľa Darwinovej teórie o predchodcoch človeka) nie sú vytvorené u iných živočíchov na zemi. Táto skutočnosť v praktickej kriminalistike vedie k tomu, že nájdené daktyloskopické stopy je možné jednoznačne prisúdiť človeku. [4]

3.3 Daktyloskopia

Je to náuka o obrazcoch papilárnych línií na vnútornej strane článkov prstov, na dlaniach a chodidlách. Daktyloskopia sa zaoberá využitím odtlačkov prstov pre identifikáciu osôb. Možnosť využitia papilárnych línií pre identifikáciu sa riadi týmito tromi zákonmi [4]:

1. Zákon o nemennosti papilárnych línií

Obrazce papilárnych línií zostávajú po celý život človeka relatívne nemenne. Papilárne línie sa začínajú tvoriť v prenatálnom štádiu, a to už v štvrtom mesiaci embryonálneho života. Tým je daný základ kresby papilárnych línií, ktorý je zachovaný v nezmenenej podobe počas celého života. Pokusy v ktorých boli porovnávané odtlačky jednej a tej istej osoby v dlhoročných odstupoch preukázali, že obrazce sú nemenné, so všetkými svojimi charakteristickými znakmi, len vo vysokom veku sú niekedy narušené vráskami.

2. Zákon o neodstrániteľnosti papilárnych línií

Papilárne línie sú relatívne neodstrániteľné, pokiaľ nie je odstránená aj zárodočná vrstva kože. Spálením, odrezaním alebo zrezaním povrchovej vrstvy kože nie je možné papilárne línie natrvalo odstrániť. To je možné jedine v prípade ak by bola odstránená aj zárodočná vrstva kože. Odstránenie alebo poškodenie vrchnej časti kože, ktoré spôsobí odstránenie papilárnych línií je len dočasné.

3. Zákon o individuálnosti papilárnych línií

nie sú na svete dvaja jedinci, ktorý by mali rovnaké obrazce papilárnych línií. Jednoduchý výpočet predpokladajúci existenciu len dvadsiatich papilárnych línií na jednom poslednom článku prstu ukazuje, že je teoreticky možných asi 64 miliárd rôznych obrazcov. Toto veľmi vysoké číslo svedčí o tom, že výskyt dvoch úplne totožných kresieb u rôznych osôb je vysoko nepravdepodobný. Preto je daktyloskopický obrazec považovaný pre potreby kriminalistiky za dostatočne individuálny

Jedinečnosť odtlačkov

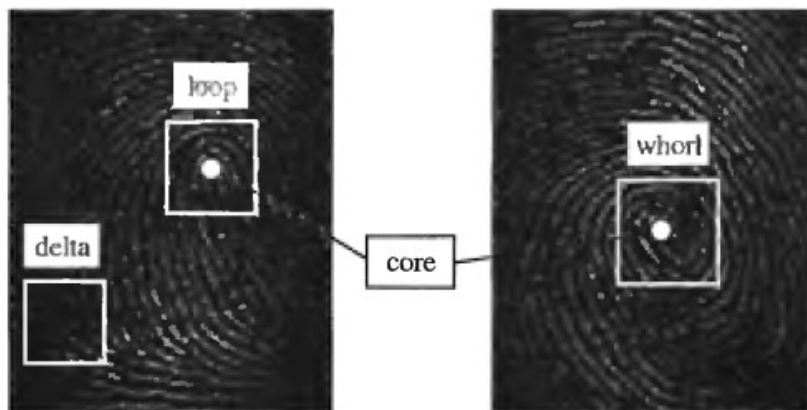
Aj keď je jedinečnosť odtlačkov prstov vnímaná ako fakt a synonymum individuality, nejedná sa o fakt ale o výsledok empirického skúmania. [1]

3.4 Špecifické znaky odtlačku.

Singulárne body

Každý odtlačok prstu je usporiadaný v určitom globálnom tvare, ktorý je daný polohou a počtom singulárnych bodov. Sú dva typy singulárnych bodov. Označujú sa ako jadro a delta. Jedná sa o miesta so zvýšeným výskytom zakrivených papilárnych línií. Pokiaľ by boli papilárne línie vrstevnice tak by

bolo jadro najvyšším bodom, teda vrcholom, tvorí ho buď slučka alebo vír. Delta je bod z ktorého papilárne línie vystupujú do troch rôznych smerov(Obrázok 3.2).[1]



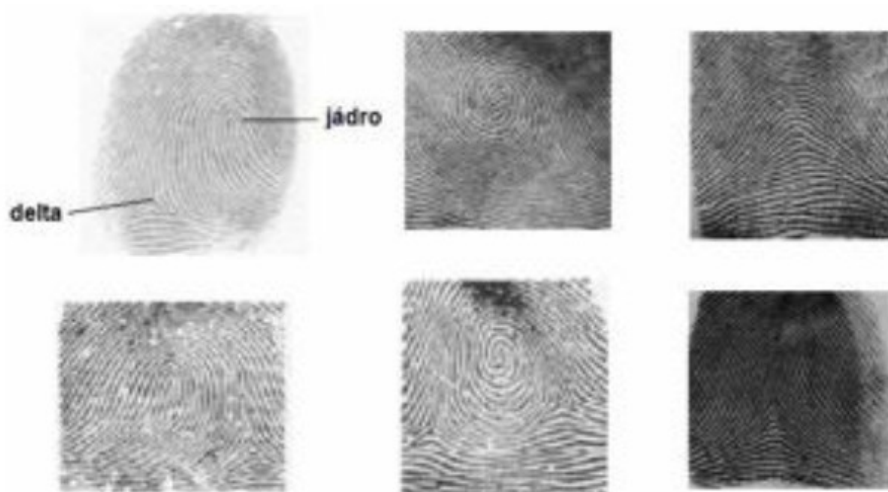
Obrázok 3.2 Jadro a delta odtlačku.[1]

V celosvetovej praxi sa daktyloskopický odborníci zhodujú na troch klasifikačných triedach (Obrázok 3.3) [9].

Oblúk – papilárne línie tu vytvárajú jednoduché oblúky. Je to najmenej častým javom na odtlačku. Oblúk sa nachádza na asi 10 % odtlačkov.

Slučka - papilárne línie vytvárajú slučku a medzi stredom centrálnej oblasti a deltou sa musí nachádzať aspoň jedna línia. Slučka sa nachádza približne na 65 % odtlačkov.

Vír – papilárne línie tu vytvárajú kruh, oval , špirálu s jadrom. Vír tvorí približne 25 % všetkých



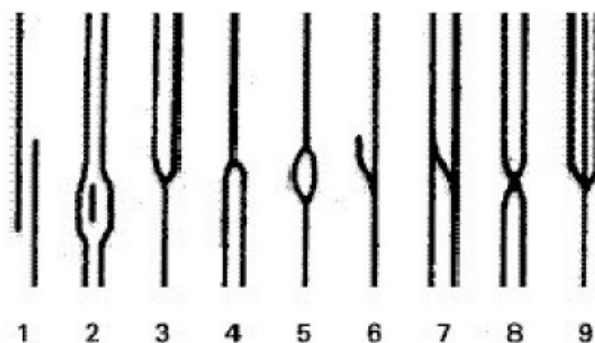
odtlačkov.

Obrázok 3.3Klasifikačné triedy: zľava slučka vír, oblúk [9]

Československá a neskôr aj česká klasifikácia bola založená na šiestich klasifikačných triedach, oblúk, otvorená slučka vľavo, otvorená slučka vpravo, viac násobný deltový vzor, uzavretá slučka vľavo, uzavretá slučka vpravo. Niektoré zahraničné klasifikácie používajú dokonca 9 klasifikačných vzorov. Klasifikácia odtlačkov je výhodná pre zníženie množstva odtlačkov pre porovnávanie. Jednotlivé odtlačky sú porovnávané len s tými, ktoré patria do rovnakej klasifikačnej triedy.[4]

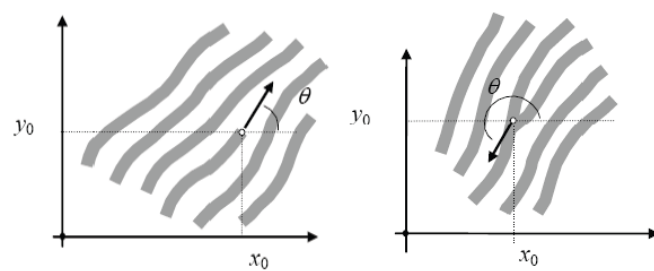
Markanty

Z fyziologického hľadiska je odtlačok prsta konfigurácia záhybov, ktoré obsahujú individuálne póry, oddelené priehlbínami. Markanty sú zmeny v priebehu papilárnych línii a sú ďalším charakteristickým prvkom každého odtlačku. Tieto znaky v odtlačku sú nositeľmi jedinečnosti odtlačkov prstov a každý odtlačok ich má niekoľko desiatok. Vo forenznej sfére sa rozlišuje množstvo typov markantov (Obrázok 3.4). Bolo zistené, že každý druh markantu má určitú pravdepodobnosť s ktorou sa vyskytuje v skúmanom odtlačku.[4]



Obrázok 3.4 Typy markantov: 1 – ukončenie 2- krátka hrana 3,4 vidlica 5 – očko.[4]

V komerčných a bezpečnostných aplikáciách sú najčastejšie rozlišované len dva typy markantov – dvojityvidlica (rozdvojenie) a ukončenie (začiatok) papilárnych línii. Každý markant je jednoznačne určený svojou polohou, smerom a typom. Smery markantov majú svoj význam v mnohých porovnávajúcich algoritmoch. Orientácia markantu typu ukončenie je uhol θ , ktorý zvierá horizontálna os x s dotyčnicou markantu. Orientácia markantu typu rozdvojenie je vypočítaná ako uhol θ , ktorý zvierá horizontálna os x s dotyčnicou markantu ukončenie (Obrázok 3.5) Je zrejmé, že všetky ďalšie markanty sú tvorené určitou kombináciou ukončení a rozdvojení. Použitie len dvoch základných typov markantov pre popis odtlačkov je dôležité hlavne pre zjednodušenie procesu rozpoznávania, pretože ich detekcia je zo správne spracovaného obrazu jednoznačná a triviálna.[11] [12]



Obrázok 3.5 Markanty vidlica a ukončenie.[12]

4 Spôsoby získania odtlačkov prstov

Úspešné nasnímanie odtlačku prstu je základný predpoklad a taktiež nevyhnutná podmienka k rozpoznaniu osoby. Snímanie daktyloskopických odtlačkov podľa časovej postupnosti a technológie snímania je možné rozdeliť do dvoch základných skupín.

1. klasické snímanie daktyloskopických stôp
2. bezprostredne snímanie daktyloskopických odtlačkov

Klasické snímanie daktyloskopických stop

Jedná sa o postupy využívané kriminalistikou a policajnými službami. Súčasťou tohto procesu je vyhľadávanie, zviditeľňovanie daktyloskopických stôp, a prenášanie do daktyloskopických zbierok a evidencií.

Bezprostredné snímanie daktyloskopických odtlačkov

Bezprostredné snímanie je dnes typické pre aplikácie komerčného a bezpečnostného charakteru. Osoba, ktorá požaduje vstup do určitého objektu priloží prst k snímaciemu senzoru, ten zosníma odtlačok a v zapätí nasleduje jeho verifikácia. Pre bezprostredne snímanie je vžitý anglický termín *live-scanning*. V praxi tento termín zahrnuje všetky technológie snímania daktyloskopického odtlačku a jeho automaticky prevod do digitálnej podoby.

Snímače môžeme rozdeliť do dvoch základných skupín podľa typu snímania odtlačku:

- **kontaktné senzory**
- **bezkontaktné senzory**

podľa typu senzora, ktorý obsahuje čítačka odtlačkov ich je možné rozdeliť na tieto typy

- **optické**
- **polovodičové**
- **ultrazvukové**

existujúce snímače je možné zaradiť do jednej z týchto dvoch kategórií

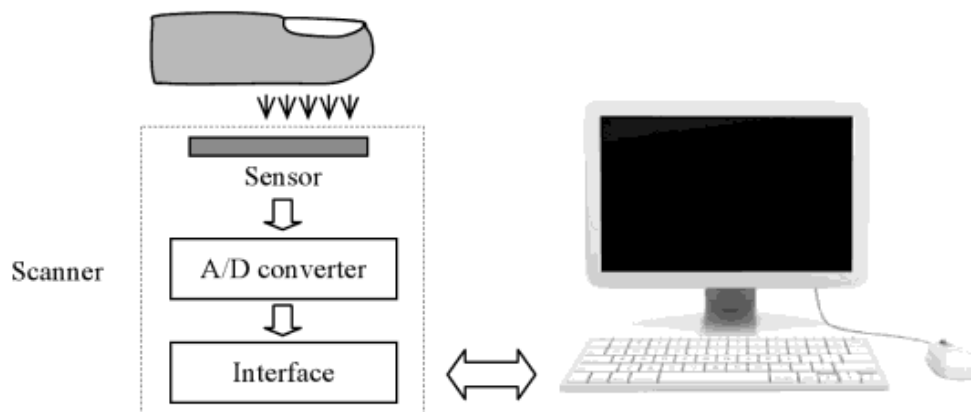
- **Multi-finger**

V jednom okamihu môže byť zosnímaný viac ako jeden prst. Zvyčajne sú snímané 4 prsty na ruke okrem palca.

- **Single-finger**

Zosnímaný je len jeden odtlačok. Tieto snímače sú široko používané v komerčných a osobných aplikáciách pre svoju cenovú dostupnosť a jednoduchosť použitia.

Na obrázku (Obrázok 4.1) je zobrazená štruktúra typického snímača odtlačkov prstov (scanner). Zosníma štruktúru papilárnych línií z priloženého prstu a A/D prevodníkom (A/D converter) prevedie analógový signál do digitálnej podoby. Rozhranie (Interface) komunikuje s ďalším externým zariadením (osobný počítač, server,...).



Obrázok 4.1 Blokový diagram čítačky odtlačkov.[1]

Snímače môžeme deliť taktiež podľa spôsobu snímania obrazu odtlačku.

- **Statický :**

snímač bude mať taký rozmer, aby dokázal zosnímať na jeden krát celý prst sa priloží na tento snímač a po určitom čase sa vytvorí snímok odtlačku.

Výhoda: snímka odtlačku sa vyhotoví počas jednej operácie.

Nevýhoda: zbytočne veľká plocha, potrebná na zosnímanie odtlačku.

- **Postupne snímateľný :**

je použitý obdĺžnikový snímač, ktorý je širší ako šírka prsta a vysoký je niekoľko pixelov. Snímanie prebieha postupným potiahnutím prsta cez tento snímač. Odtlačok je nasnímaný a rozdelený do viacerých častí a tieto sú potom zrekonštruované a spojené do jedného celku pomocou programu

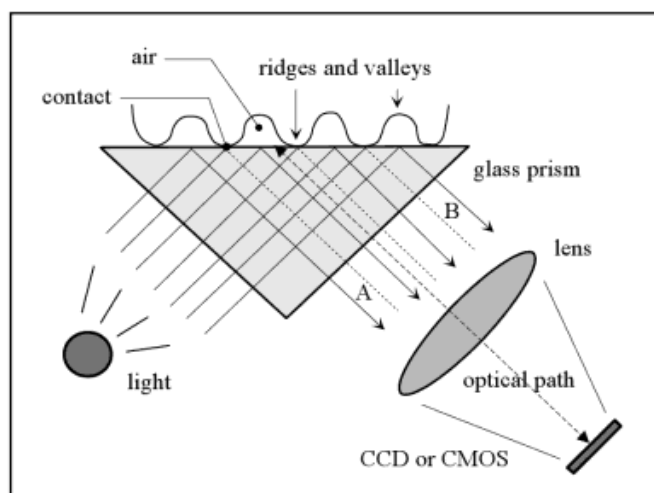
Výhoda: malý rozmer a určité samočistiace vlastnosti, nízka výrobná cena po zosnímaní na snímači nezostáva žiaden zvyškový odtlačok

Optické snímače:

FTIR (Frustrated Total Internal Reflection)

V súčasnosti je to najpoužívanější spôsob snímania odtlačku prstu. Prst sa dotýka skleneného alebo plastového povrchu. Vrcholy papilárnych línií sú v priamom kontakte s povrchom, údolia papilárnych línií zostávajú v určitej vzdialenosti. Do jednej strany hranolu vniká difúzne svetlo ktoré je eliminované sadou LED diód. Toto svetlo dopadá na hranol a prst, a je buď odrazene na CCD (CMOS) senzor alebo je rozptýlené (absorbované údoliami papilárnych línií) (Obrázok 4.2). Výstupný obraz je v stupňoch šedej. Vchody papilárnych línií sú v tmavých odtieňoch a údolia reprezentujú svetlé miesta vo výstupnom obraze. Keďže FTIR snímajú trojrozmerný povrch priloženého prstu nie je ich možné tak jednoducho oklamať napr. priloženou fotografiou .

Pri týchto snímačoch môžu nastať problémy so snímaním veľmi suchých prstov. Niektoré snímače sú vybavené silikónovou fóliou, ktorá zlepšuje kvalitu snímku veľmi suchých prstov a zabraňuje fyzickému poškodeniu snímacej plochy. Výhodou týchto snímačov je dostatočne veľká snímacia plocha , dobré rozlíšenie a dobrá kvalita obrazu. Sú predovšetkým vhodné pre porovnávacie algoritmy založené na markantoch[7].

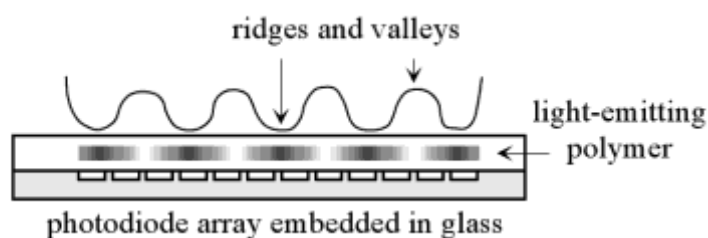


Obrázok 4.2 Snímanie technológiou FTIR.[1]

Elektro-optické snímače

Tieto zariadenia sa skladajú z dvoch hlavných vrstiev. Prvá vrstva dokáže emitovať svetlo ak je polarizovaná pod správnym napätím. Hrebene papilárnych línií sú vo fyzickom kontakte s polymérom a údolia nie, to spôsobuje, že potenciál nie je rovnaký na celej ploche priloženého prstu. Tým pádom sa mení aj svetlo emitované polymérom podľa dotyku papilárnych línií s polymérom. Druhá časť je zložená z fotodiódy vlozenej do skla, ktorá je zodpovedná za prijímanie svetla z polyméru a jeho

premeny na digitálny obraz (Obrázok 4.3). Niektoré senzory obsahujú len prvú vrstvu emitujúcu svetlo a štandardný objektív a CMOS senzor pre získanie a digitalizáciu obrazu. Aj napriek veľkej miniaturizácii týchto snímačov, snímky získané touto technológiou majú porovnateľne horšiu kvalitu ako snímky získané pomocou FTIR .



Obrázok 4.3 Elektro optický snímač.[1]

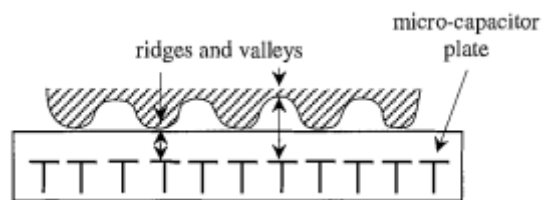
Polovodičové snímače

Polovodičové snímače (tiež známe ako kremíkové snímače). Tieto senzory boli navrhnuté pre prekonanie cenovej nedostupnosti optických senzorov. V osemdesiatych a deväťdesiatych rokoch sa to zdalo ako bariéra pre nasadenie systémov rozpoznávajúcich odtlačky prstov. V skutočnosti cena kremíkových senzorov nie je o nič nižšia ako cena optických, a obzvlášť ak majú malú snímaciu plochu nie je táto cena prípustná. Všetky senzory na báze kremíka sú zložené z poľa pixlov a každý pixel sám o sebe tvorí malý senzor. Užívateľ sa priamo dotýka jeho povrchu a nie sú potrebné komponenty ako CCD alebo CMOS senzor.

Kapacitne snímače

Sú to najpoužívanjšie polovodičové snímače, pracujúce na princípe mikrokondenzátorov. Snímač obsahuje pole usporiadaných mikroelektrod. Druhú časť mikro kondenzátorov tvorí priložená koža prstu. Medzi kožou a mikroelektrodami vzniká elektrický náboj, jeho veľkosť závisí na vzdialenosti prstu od dosiek mikrokondenzátora. Vzdialenosť vrcholov papilárnych línií od vrstvy s mikroelektrodami je menšia ako vzdialenosť mikroelektrod od údolí papilárnych línií. Rozdiel v týchto vzdialenostiach spôsobí aj rozdiel vo vzniknutom elektrickom náboji (Obrázok 4.4). Veľkosť elektrických nábojov potom určí hodnotu jednotlivých pixlov vo výstupnom obraze.

Kapacitne snímače nie sú oklamateľné priložením fotografie odtlačku, pretože pracujú na princípe merania vzdialenosti trojrozsomernej plochy. Nevýhodou je že časte čistenie povrchu snímača, pretože nečistoty spôsobujú zmenu výsledného obrazu.



Obrázok 4.4 Princíp funkcie kapacitného snímača.[1]

Teplotné snímače

Využívajú princíp merania rozdielu teploty kože a vzduchu zachyteného v papilárnych líniách. Je nutné prejsť prstom po ploche snímača. Obraz je snímaný postupne po obdĺžnikoch o veľkosti plochy senzora. Výsledný obraz je zložený z týchto čiastočných obrazov odtlačku. Senzor dokáže rozpoznať pravý prst od neživej napodobeniny avšak výstupný obraz nie je veľmi kvalitný. Tieto snímače sú realizované ako postupne snímajúce, realizácia teplotného dotykového snímača je nevhodná, pretože po priložení dochádza k rýchlemu vyrovnaniu teplotných rozdielov, čo by malo za následok odlišný obraz. Je náchylný k chybám, pretože nečistoty na prste môžu spôsobiť chybný výsledný obraz, taktiež potrebuje istú údržbu, pretože tieto nečistoty ostávajú na skenovacej ploche.

Tlakový snímač

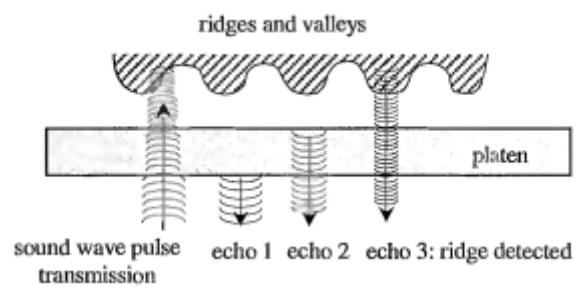
Tieto snímače sú navrhnuté tak aby generovali elektrický signál, keď na ne pôsobí mechanický tlak. Povrch je vyrobený z nevodivého izolačného materiálu, ktorý pod tlakom vytvára malé množstvo elektrického prúdu. Keďže údolia a vrcholy papilárnych línií sú v rôznej vzdialenosti, pri snímaní bude u nich vytvorený odlišný prúd.

Tieto zariadenia poskytujú binárny obraz obsahujúci minimálnu informáciu. Tento spôsob je však dosť nevhodný z dôvodu nízkej citlivosti a vďaka neschopnosti rozlíšiť medzi živým a umelým prstom.

Ultrazvukové snímače:

Ultrazvukové snímače pracujú na princípe merania vzdialenosti od zdroja pomocou akustických vĺn. Technológia funguje na podobnom princípe ako radar. Jeho výhodou je, že ultrazvuk ľahko prenikne nečistotami, ktoré by ináč znehodnotili obraz. Snímač sa skladá z vysielača, ktorý posiela impulzy a prijímača, ktorý získava odrazy týchto vĺn. Rozdiely v prijatých vlnách sú premietnuté do výsledného obrazu, zobrazujú rozdiely vzdialenosti medzi údoliami a vrcholmi papilárnych línií (Obrázok 4.5).

Takéto snímanie ponúka veľmi kvalitný obraz, avšak tieto prístroje sú pomerne veľké a drahé, navyše trvá získanie obrazu až niekoľko sekúnd.



Obrázok 4.5 Princíp fungovania ultrazvukového snímača.[1]

5 Predspracovanie obrazu odtlačku

Úspešnosť algoritmov, ktoré pracujú na základe porovnávania orientácii a polohy markantov sú značne závislé na kvalite vstupného obrazu. Úspešnosť a presnosť extrakcie markantov je priamo závislá na kvalite vstupného obrazu. V ideálnom prípade sú údolia a hrebene papilárnych línií pravidelne striedane a vedené rovnakým smerom, čo umožňuje veľmi presne a jednoznačne získanie markantov. Reálny odtlačok môže byť v zhoršenej kvalite, ktorá je spôsobená stavom pokožky snímaného prsta (suchá, vlhká, poškodenie, vrásky), veľmi nízkym alebo veľmi silným tlakom pri priložení prsta k snímaču odtlačkov alebo veľmi nízkou kvalitou samotného prstu (manuálne pracujúci ľudia, poškodenie vekom) (Obrázok 5.1). V praxi je kvalita zosnímaného obrazu priamo závislá na kvalite snímacieho zariadenia a výstupe obrazu, ktorý tento snímač poskytuje. Preto sú pred vyhľadávaním markantov v odtlačkoch aplikované metódy na zníženie šumu v obraze a pre zvýraznenie rozdielov medzi údoliami a vrcholmi papilárnych línií. [1][11]



Obrázok 5.1 Odtlačok prsta a) vo veľmi dobrej kvalite b) v strednej kvalite c) v zlej kvalite.[1]

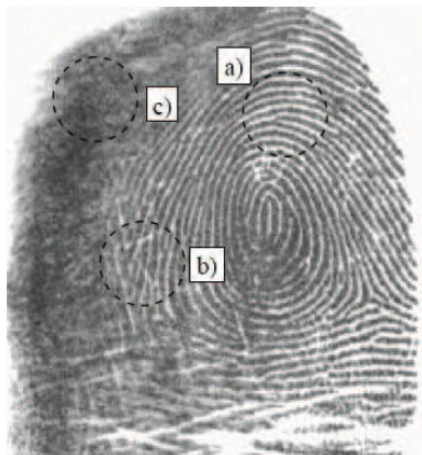
Môžeme hovoriť o niekoľkých poruchách, ktoré sú spôsobené zlou kvalitou vstupného obrazu:

- hrebene papilárnych línií sú prerušené na jednom alebo viacerých miestach,
- zle oddelenie papilárnych línií spôsobené šumom medzi líniami,
- vrásky, odreniny a jazvy.

Tieto poruchy spôsobujú, že detekcia markantov vo veľmi poškodených oblastiach je obtiažna a má to za následok tieto problémy

- je detekované veľké množstvo falošných markantov,
- nie je detekované veľké množstvo pravých markantov,
- chybovosť a nepresnosť v detekcii orientácie, typu a umiestnenia markantov.

Preto je potrebné na odtlačky aplikovať postupy zlepšujúce kvalitu obrazu, čo vedie k správnej detekcii markantov. Tieto postupy sú však účinné len v oblastiach odtlačku s aspoň minimálnou informáciou o papilárnych líniách. Plocha odtlačku môže byť rozdelená do troch oblastí (Obrázok 5.2)



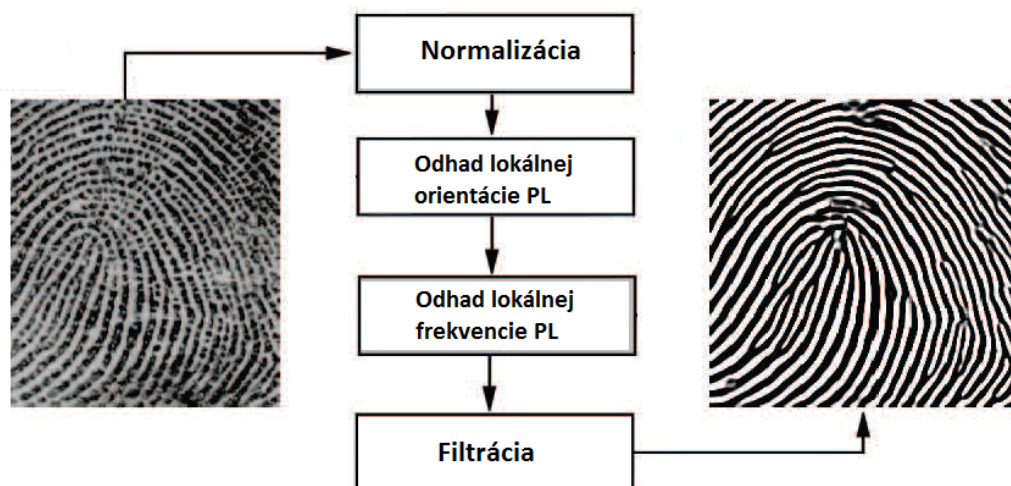
Obrázok 5.2 Kategórie oblastí a) dobre rozpoznateľná oblasť b) obnoviteľná oblasť c) neobnoviteľná oblasť. [1]

5.1 Gaborova filtrácia

Jedna z najcitovanejších metód pre vylepšenie kvality odtlačku prsta je metóda použitá L. Honom,[14] ktorá je založená na konvolúcii obrazu s Gaborovými filtermi a vychádza z lokálnych charakteristík odtlačku, zo smeru a frekvencie hrebeňov papilárnych línií. Táto metóda pozostáva zo štyroch základných krokov (Obrázok 5.3)[1]:

1. Normalizácia.
2. Výpočet orientácií papilárnych línií.
3. Výpočet frekvencií papilárnych línií.
4. Filtrácia bankou Gaborových filtrov.

K týmto krokom pre vylepšenie kvality obrazu boli pridané v praktickej realizácii segmentácia popredia obrazu od pozadia a vytvorenie kostry obrazu[11].



Obrázok 5.3 Výstup jedného podprocesu je vstupom ďalšieho procesu. upravené z [1].

Segmentácia

Prvým krokom algoritmu pre vylepšenie kvality obrazu je segmentácia obrazu. Segmentácia je proces oddelenia regiónov pozadia obrazu od jeho popredia. Popredie obrazu tvoria regióny s hrebeňmi a údoliami papilárnych línií, ktoré predstavujú oblasť záujmu. Keby bol algoritmus pre rozpoznávanie markantov aplikovaný na pozadie tak by jeho výsledkom bolo veľké množstvo falošných markantov. Preto ma segmentácia za následok presnejšiu extrakciu markantov.

Pozadie obrazu tvoria oblasti mimo zosnímaného odtlačku prsta. Popredie obrazu vykazuje veľký rozptyl šedej a pozadie veľmi nízky rozptyl, preto je možné vykonať segmentáciu popredia od pozadia prahovaním. Najprv je obraz rozdelený do blokov $W \times W$ a rozptyl šedej je vypočítaný pre každý blok. Ak je hodnota rozptylu menšia ako globálny prah, tak je blok označený ako región pozadia.

$$V(k) = \sum_{i=0}^{W-1} \sum_{j=0}^{W-1} (I(i,j) - M(k))^2,$$

kde $V(k)$ je rozptyl v bloku k , $I(i,j)$ je úroveň šedej v mieste (i,j) a $M(k)$ je prevažujúca úroveň šedej v bloku [1][11].

Normalizácia

Normalizácia je proces úpravy hodnôt pixelov do požadovaného rozsahu, nemení štruktúru papilárnych línií. Účelom normalizácie je štandardizácia hodnôt v úrovni šedej, ktorá uľahčuje vykonanie ďalších fáz pre spracovanie obrazu. Výpočet normalizovaného obrazu definuje rovnica (2). Úroveň šedej v bode (i,j) reprezentuje hodnota $I(i,j)$. $N(i,j)$ je normalizovaná hodnota pixelu (i,j) ,

M je stredná hodnota vypočítaná z obrazu I , V je variácia $I(i, j)$. M_0 je požadovaná hodnota V_0 je požadovaná hodnota variácie.

$$M(i, j) = \begin{cases} M_0 + \sqrt{\frac{V_0(I(i, j) - M)^2}{V}} & \text{ak } I(i, j) > M \\ M_0 - \sqrt{\frac{V_0(I(i, j) - M)^2}{V}} & \text{inak} \end{cases}$$

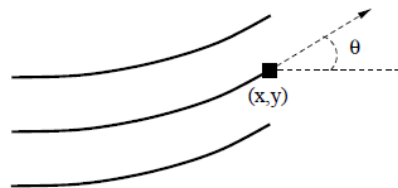
$$M(I) = \frac{1}{W^2} \sum_{i=0}^{W-1} \sum_{j=0}^{W-1} I(i, j)$$

$$V(I) = \frac{1}{W^2} \sum_{i=0}^{W-1} \sum_{j=0}^{W-1} (I(i, j) - M(I))^2$$

Výpočet orientácií papilárnych línií

Odhad orientácii je základným krokom v procese vylepšenia obrazu Gaborovou filtráciou, ktorá sa spolieha na výpočet orientácie papilárnych línií. K výpočtu obrazu orientácii papilárnych línií je používaná metóda výpočtu v najmenšom štvorci, Metoda výpočtu orientácie pre pixel však ponúka jemnejší a presnejší odhad orientovaného poľa.

Lokálna orientácia papilarnej línie je uhol θ_{xy} , ktorý je zvieraný horizontálnou osou a dotyčnicou papilarnej línie v bode (x, y) (Obrázok 5.4). Keďže papilárne línie nemajú svoj smer nijak definovaný, uhol θ_{xy} dosahuje hodnôt $< 0, 180 >$. Smerový obraz odtlačku je matica M , ktorej prvky sú lokálne orientácie papilárnych línií.[11]



Obrázok 5.4 Orientácia papilárnej línie v bode.[12]

Kroky výpočtu orientovaného obrazu sú nasledovné [11]:

1. V normalizovanom obraze je okolo pixelu (i, j) vycentrovaný blok o veľkosti $W \times W$
2. Pre každý pixel v bloku sú vypočítané gradienty $\partial_x(i, j)$ a $\partial_y(x, y)$, ktoré sú veľkosťami gradientov v smeroch x a y .

Horizontálny sobelov operátor je použitý pre výpočet gradientu ∂_y .

$$\begin{bmatrix} 1 & 0 & -1 \\ 2 & 1 & -2 \\ 1 & 0 & -1 \end{bmatrix}$$

Vertikálny sobelov operátor je použitý pre výpočet gradientu ∂_x .

$$\begin{bmatrix} 1 & 2 & 1 \\ 2 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix}$$

3. Lokálna orientácia pixelu (i, j) je vypočítaná ako:

$$V_x(i, j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} 2\partial_x(u, v)\partial_y(u, v),$$

$$V_y(i, j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} \partial_x^2(u, v)\partial_y^2(u, v),$$

$$\theta(i, j) = \frac{1}{2} \tan^{-1} \frac{V_y(i, j)}{V_x(i, j)},$$

kde $\theta(i, j)$ je najmenší odhad lokálnej orientácie okolo pixelu (i, j) .

4. Pre vyhladenie orientovaného obrazu v jeho najbližšom okolí je použitý Gaussov filter.

Orientovaný obraz je predtým prevedený do spojitého vektorového poľa

$$\Phi_x(i, j) = \cos(2\theta(i, j)),$$

$$\Phi_y(i, j) = \sin(2\theta(i, j)),$$

kde Φ_x a Φ_y sú zložky vektorového poľa, následné na to aplikovaný Gaussov filter

$$\Phi'_x = \sum_{u=-\frac{w_\Phi}{2}}^{\frac{w_\Phi}{2}} \sum_{v=-\frac{w_\Phi}{2}}^{\frac{w_\Phi}{2}} G(u, v)\Phi_x(i - uw, j - vw),$$

$$\Phi'_y = \sum_{u=-\frac{w_\Phi}{2}}^{\frac{w_\Phi}{2}} \sum_{v=-\frac{w_\Phi}{2}}^{\frac{w_\Phi}{2}} G(u, v)\Phi_y(i - uw, j - vw),$$

Kde G je Gaussov filter pre dolnú priepust veľkosti $w_\Phi \times w_\Phi$

5. **Výsledné** vyhladený orientovaný obraz O pixelu (i, j) je definovaný ako :

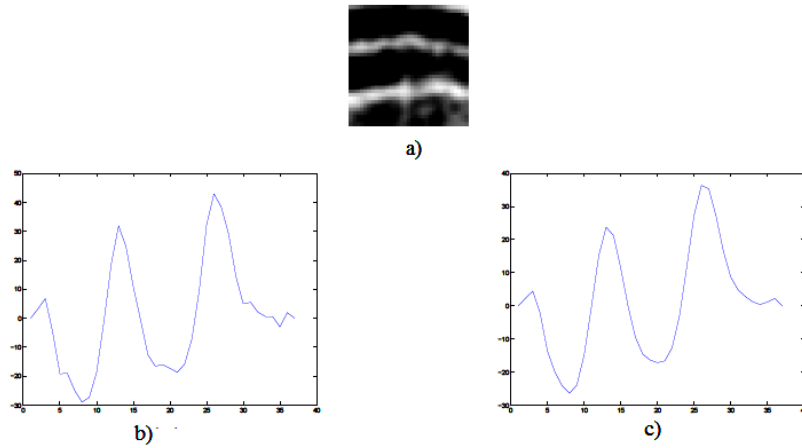
$$O(i, j) = \frac{1}{2} \tan^{-1} \frac{\Phi'_y(i, j)}{\Phi'_x(i, j)}.$$

Výpočet frekvencií papilárnych línií

Ďalší dôležitý parameter, ktorý je použitý pri konštrukcii Gaborovho filtra je lokálna frekvencia hrebeňov papilárnych línií. Výpočet frekvenčného obrazu je možné rozdeliť na dve časti. V prvej fáze odhadu frekvencie je blok rozdelený do blokov o veľkosti $W \times W$. Ďalším krokom je premietnutie hodnôt úrovni šedej umiestnených v bloku pozdĺž smeru k lokálnej orientácii hrebeňa papilárnej línie. Táto projekcia vytvára vlnu takmer sínusového tvaru. Thai [11] doplnil pôvodný výpočet vytvorený Hongom [14] o vyhladenie vyprojektovanej krivky Gaussovým filtrom pre dolnú priepusť (Obrázok 5.5). Vzdialenosť hrebeňov $S(i, j)$ je potom vypočítaná ako súčet stredných hodnôt vzdialenosti pixelov medzi dvoma susednými bodmi vo vyprojektovanej krivke. Frekvencia hrebeňa $F(i, j)$ pre blok vycentrovaný okolo pixelu (i, j) definovaná ako :

$$F(i, j) = \frac{1}{S(i, j)}.$$

Vzhľadom k tomu , že je odtlačok zosnímaný v pevne danom rozlíšení, mala by byť frekvencia hrebeňov papilárnych línií v pevne danom rozsahu. Avšak, sú prípady kedy nie je možné získať správnu frekvenciu, ako napríklad keď nie sú v bloku detekované žiadne vrcholy a taktiež pri výskyte markantov v bloku. V blokoch obsahujúcich markanty nemá vyprojektovaná krivka sínusový tvar, .To potom vedie k nepresnému odhadu frekvencií hrebeňov papilárnych línií .Tieto hodnoty sú doplnené priemerom hodnôt zo susedných blokov .V závere je získaný frekvenčný obraz vyhladený Gaussovým filtrom pre dolnú priepusť.



Obrázok 5.5 Efekt vyhladenia projekcie pre výpočet frekvencie hrebeňov papilárnych línii. a) blok s o veľkosti 32 x 32 pixelov, b) pôvodná projekcia c) vyhladená projekcia. [11]

Filtrácia bankou Gaborovych filtrov

Normalizovaný, orientovaný a frekvenčný obraz poskytujú dostatok informácii pre aplikáciu Gaborovych filtrov na normalizovaný obraz.

Účelom aplikácie týchto filtrov je zvýrazniť hrebene papilárnych línii v obraze a zároveň znížiť šum. Ku konštrukcii gáborovych filtrov je použitý obraz frekvencií hrebeňov papilárnych línii a orientovaný obraz. Gaborov filter pozostáva zo sínusovej vlny určitej orientácie a frekvencie. Tým pádom pásmová priepust účinné odstraňuje nežiaduci šum pri zachovaní štruktúry papilarnej línie. Gaborove filtre majú silne frekvenčné a smerovo selektívne vlastnosti, ktoré spôsobujú citlivosť na papilárne línie. Gaborov filter je reálnou časťou gaborovej funkcie. Gaborov filter je definovaný ako[11]:

$$G(x, y, \theta, f) = \exp\left\{-\frac{1}{2}\left[\frac{x_{\theta}^2}{\sigma_x^2} - \frac{y_{\theta}^2}{\sigma_y^2}\right]\right\} \cos(2\pi f x_{\theta}),$$

$$x_{\theta} = x \cos \theta + y \sin \theta,$$

$$y_{\theta} = -x \sin \theta + y \cos \theta,$$

kde θ je orientácia Gaborovho filtra, f predstavuje frekvenciu, σ_x a σ_y su štandardné odchýlky pozdĺž x a y , x_0 a y_0 definujú osy x a y v súradnicovej sústave. Konvolúcia pixelu (i, j) v obraze vyžaduje odpovedajúcu orientáciu $O(i, j)$ a frekvenciu $F(i, j)$ pixelu. Vylepšený obraz $E(i, j)$ je získaný aplikáciou filtra G :

$$E(i, j) = \sum_{u=-\frac{w_x}{2}}^{\frac{w_x}{2}} \sum_{v=-\frac{w_y}{2}}^{\frac{w_y}{2}} G(u, v, O(i, j), F(i, j)) N(i - u, j - v),$$

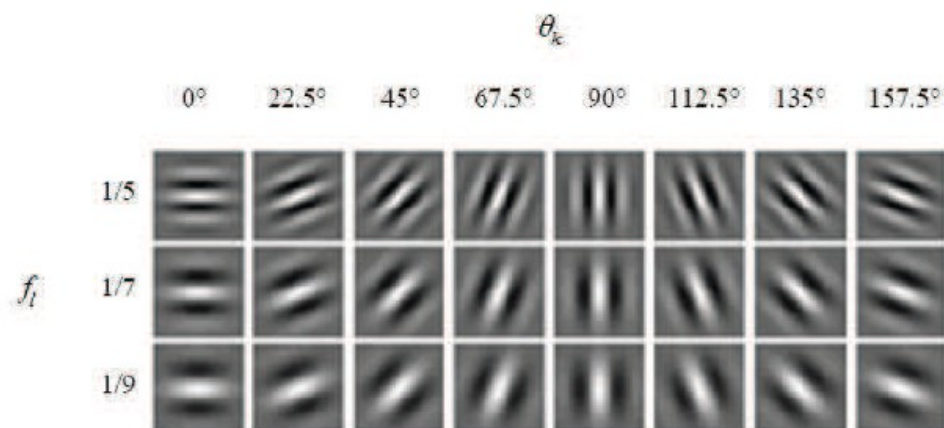
kde O predstavuje orientovaný obraz, F je frekvenčný obraz, N je normalizovaný obraz, a w_x a w_y sú šírka a výška masky Gaborovho filtra. Šírka pásma filtra, ktorá špecifikuje rozsah frekvencií filtra je ovplyvnená parametrami odchýlok σ_x a σ_y , tie sú definované ako funkcia frekvencie:

$$\sigma_x = k_x F(i, j),$$

$$\sigma_y = k_y F(i, j),$$

Kde F je frekvenčný obraz hrebeňov, k_x a k_y predstavujú konštantné premenné pre σ_x a σ_y .

Namiesto výpočtu Gaborových filtrov pre každý pixel samostatne „za letu“ je pre urýchlenie procesu vytvorená banka Gaborových filtrov. Táto je vypočítaná pred vylepšovaním obrazu a je aplikovaná na všetky odtlačky. Banka filtrov je preddefinovaná počtom diskretných orientácií a počtom diskretných frekvencií. Potom je na každý pixel (i, j) normalizovaného obrazu aplikovaný filter, ktorý je čo najbližšie orientácii a frekvencii pixelu (i, j) (Obrázok 5.6) [1].



Obrázok 5.6 Banka Gaborových filtrov. [1]

Binarizácia

Väčšina algoritmov pre extrakciu markantov pracuje s binárnym obrazom, v ktorom existujú len dve oblasti záujmu. Čierne pixely reprezentujú hrebene papilárnych línii a biele pixely predstavujú údolia papilárnych línii a pozadie obrazu. Binarizácia je proces pri ktorom sú šedo tónové hodnoty obrazu konvertované do binárneho obrazu. Tým je zvýraznený kontrast medzi hrebeňmi a údoliami papilárnych línii, čo uľahčuje a zjednodušuje extrakciu markantov.

Užitočná vlastnosť Gaborovej filtrácie je, že výsledný obraz má jednosmernú zložku nulovú, to znamená, že aj výsledný obraz má strednú hodnotu pixelov rovnú nule. Preto je jednoduché získať binárny obraz pomocou globálneho prahu s hodnotou nula. Každý pixel je porovnaný s globálnym prahom a ak je jeho hodnota väčšia ako globálny prah je mu pridelená hodnota 1. V opačnom prípade je mu pridelená hodnota 0.

Skeletizácia binárneho obrazu

Vstupom do tohto algoritmu je binárny obraz s hodnotami 0 alebo 1. Hodnoty 1 predstavujú hrebene papilárnych línií a hodnoty 0 pozadie obrazu a údolia papilárnych línií, ktoré sú pre ďalšie spracovanie nezaujímavé. Algoritmus je rozdelený na parnú a nepárnu iteráciu, aby nedochádzalo k výraznému posunutiu vytvorenej kostry obrazu. V rozložení hodnôt pixelov osem okolia je skúmané, či je možné pixel v strede odstrániť (Obrázok 5.7). Cieľom tohto procesu je stenčiť hrúbku papilárnych línií na jeden pixel bez prerušenia kontinuity hrebeňa.

q_4	q_3	q_2
q_5	q_0	q_1
q_6	q_7	q_8

Obrázok 5.7 Okolie bodu.

Aby bol bod q_0 označený ako kandidát na odstránenie musí spĺňať nasledujúce podmienky [15]:

1. Počet neprázdnych bodov v okolí nesmie byť 1.

$$N(q_0) \neq 1, kde$$

$$N(q_0) = \sum_{k=1}^8 q_k.$$

2. Prechodové číslo

$$X = \sum_{k=1}^8 |q_{k+1} - q_k|$$

musí byť $X=0,2$ alebo 4. Hodnota 0 znamená, že ide o izolovaný bod alebo bod v rámci objektu, 2 vyjadruje pozíciu na hranici objektu a 4 znamená, že sa jedná o výbežok široký jeden pixel a situáciu je potrebné podrobnejšie preskúmať v podmienkach 3 resp. 4, ktoré pomocou logických operátorov vyjadrujú akceptovateľné pozície pixelov pre odstránenie

3. Tato podmienka je aplikovaná v nepárnych iteráciách

$$(q_1 \wedge q_3 \wedge q_5) = 0 \text{ a } (q_1 \wedge q_3 \wedge q_7) = 0.$$

Pokiaľ $X=4$, potom musí byť splnená ešte jedna z podmienok a alebo b

$$\text{a) } (q_1 \wedge q_7) = 1 \wedge (q_2 \vee q_6 = 1) \wedge (q_3 \wedge q_4 \wedge q_5 \wedge q_8 = 0)$$

$$\text{b) } (q_1 \wedge q_3) = 1 \wedge (q_4 \vee q_8 = 1) \wedge (q_2 \wedge q_5 \wedge q_6 \wedge q_7 = 0)$$

4. Táto podmienka je aplikovaná v párných iteráciách

$$(q_1 \wedge q_5 \wedge q_7) = 0 \text{ a } (q_3 \wedge q_5 \wedge q_7) = 0.$$

Pokiaľ $X=4$,potom musí byť splnená ešte jedna z podmienok c alebo d

$$\text{c) } (q_3 \wedge q_5) = 1 \wedge (q_2 \vee q_6 = 1) \wedge (q_3 \wedge q_4 \wedge q_7 \wedge q_8 = 0)$$

$$\text{d) } (q_5 \wedge q_7) = 1 \wedge (q_4 \vee q_8 = 1) \wedge (q_2 \wedge q_3 \wedge q_5 \wedge q_6 = 0)$$

6 Analýza odtlačku

6.1 Hľadanie a označenie markantov

Markanty v obraze odtlačku sú určené pre ich porovnávanie, a úspešnosť tohto procesu je priamo závislá na ich presnom nájdení. Metódy detekcie markantov je možné rozdeliť podľa druhu obrazu s ktorým pracujú na:

- Metódy pracujúce s binárnym obrazom
- Metódy pracujúce v šedo tónovom obraze
-

Metódy pracujúce s binárnym obrazom

[1]

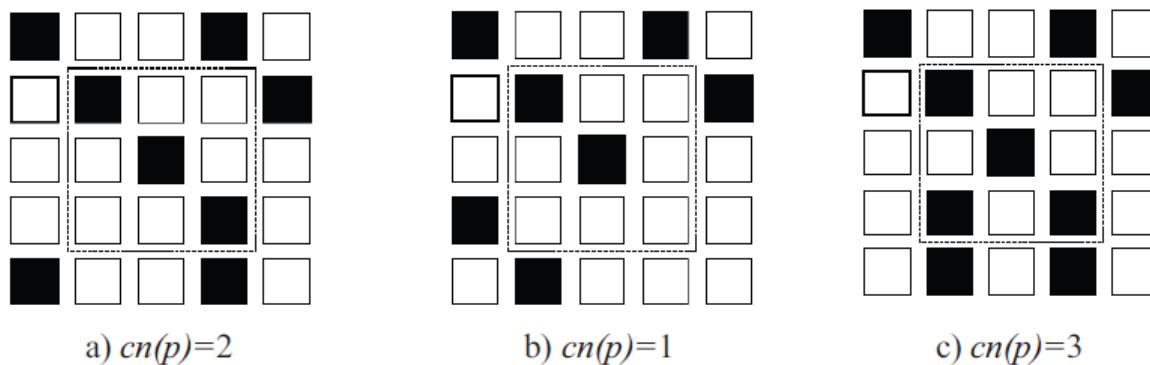
V kostre obrazu nie je nájdenie markantov veľmi zložitý. Metóda pre detekciu markantov je založená na sčítaní rozdielov medzi dvojicami v osem okolí bodu. Jedná sa o prechodové číslo (*crossing number*)

$$cn(p) = \frac{1}{8} \sum_{i=1}^8 |val(P_{i \bmod 8}) - val(P_{i-1})|,$$

keď body $P[i]$ sú body tvoriace osemokolie pixelu a $val(P)$ je hodnota pixelu. Podľa vypočítanej hodnoty prechodov sa rozhodne, či sa jedná o markant a akého je typu. Hodnota prechodového čísla je braná v úvahu len v prípade ak je hodnota pixelu pre ktorý je počítaná rovná jednej (hrebeň papilárnej línie). Môžu nastať rôzne typy výsledkov, ktoré určujú či sa jedná o markant poprípade akého je typu (Obrázok 6.1):

- $Cn(p)=1$, pixel sa nachádza na v priebehu papilárnej línie, nejedná sa o marknat.
- $Cn(p)=2$, pixel odpovedá markantu typu ukončenie(začiatok).
- $Cn(p)=3$, pixel odpovedá markantu typu vidlica (rozdzvojenie).
- $Cn(p)>3$, jedna sa o zložitejší typ markantu.

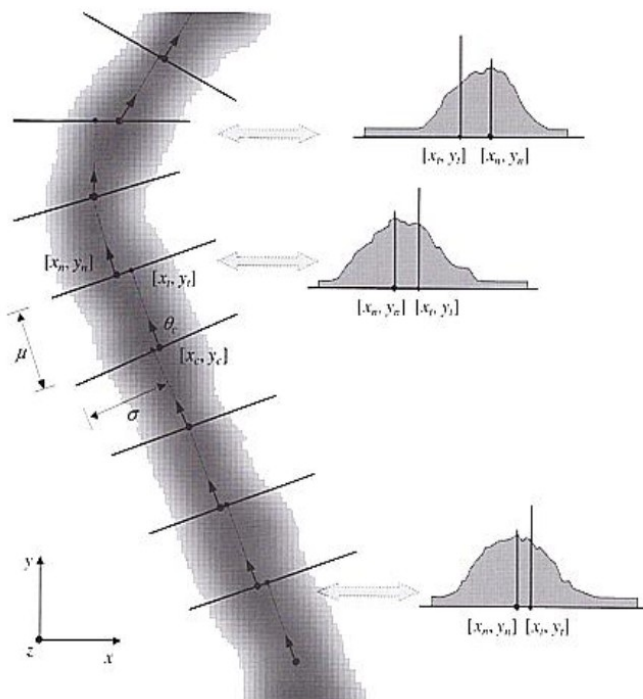
Ako bolo popísané v predchádzajúcich kapitolách, väčšina automatických systémov pracuju s markantami rozdzvojenie a ukončenie, preto sú iné hodnoty ako $cn(p)=1$ a $cn(p)=2$ nezaujímavé.



Obrázok 6.1 Rôzne konfigurácie pixelov v okolí bodu. [1]

Metódy pracujúce v šedotónovom obraze

Hrebeň papilarnej línie je sledovaný na základe lokálnej orientácie. Počiatočné informácie sa získavajú rozdelením obrazu na štvorce o strane w . Majme počiatočný bod $[x_c, y_c]$ a počiatočný smer θ_c . V každom kroku algoritmus spočíta nový bod $[x_t, y_t]$ posunutím o μ pixelov z $[x_c, y_c]$ v smere θ_c . Potom vypočíta sadu Ψ , čo je sada pixelov so stredom v bode $[x_t, y_t]$ a smerom kolmým k θ_c . Dĺžka Ψ je $2\theta + 1$. Nový bod $[x_n, y_n]$, ktorý leží na hrebeni je vybratý ako lokálne maximum Ψ . Bod $[x_n, y_n]$ sa stáva novým počiatočným bodom $[x_c, y_c]$ a vypočíta sa nový smer θ_c (Obrázok 6.2).[1]

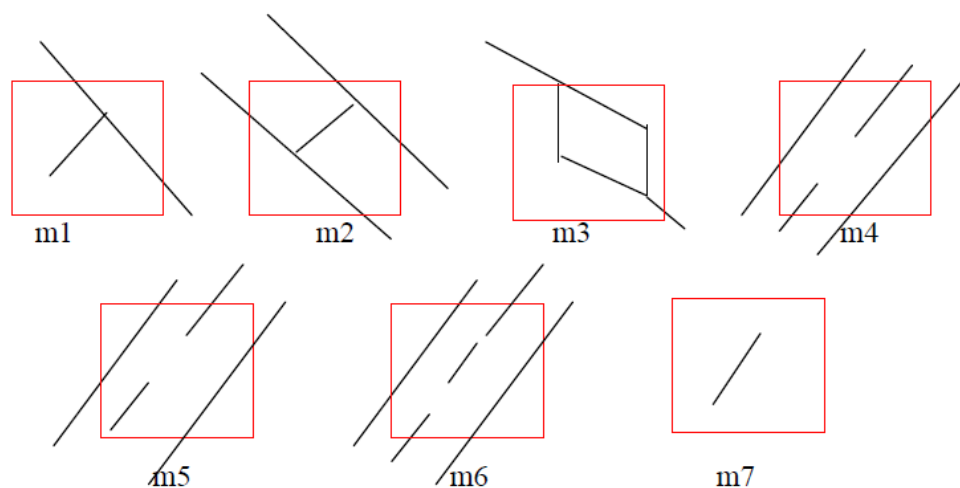


Obrázok 6.2 Niektoré kroky metódy sledovania hrebeňa. [1]

Algoritmus pokračuje pokiaľ nie je splnená jedna zo štyroch podmienok ukončenia. Pokiaľ je línia hrebeňa ukončená, alebo pretína inú líniu, algoritmus sa zastaví a vráti pozíciu a typ markantu. Detailný popis algoritmu sa nachádza v [1].

Odfiltrovanie falošných markantov

Gáborovou filtráciou sa značne vylepší kvalita obrazu, čo má za následok presnejšiu detekciu markantov avšak stále je detekované veľké množstvo falošných markantov. Niekedy sú vytvorené artefakty, ktoré sú dôsledkom predpracovania odtlačku (Obrázok 6.3). Tieto markanty priamo ovplyvňujú úspešnosť porovnávania odtlačkov. Odstránenie falošných markantov je základom úspechu pri porovnávaní odtlačkov. Preto je určených niekoľko pravidiel, ktoré tieto markanty odstraňujú metódou, ktorú popisuje Wu Zhili.[12]



Obrázok 6.3 Typy falošných markantov.[12]

Na (Obrázok 6.3) je definovaných niekoľko typov falošných markantov. Markant typu m1 je bod zasahujúci do údolia medzi dvoma papilárnymi líniami. Typ m2 predstavuje falošné prepojenie dvoch papilárnych líní, m3 je falošné spojenie dvoch vidlíc. Na m4 sa nachádzajú dva markanty typu ukončenie, podobne aj v prípade m5 ale s tým rozdielom, že je prítomné ďalšie prerušenie na jednej z papilárnych líní. M6 je veľmi podobne ako predchádzajúci prípad ale s tým rozdielom, že sa medzi dvoma líniami nachádza ďalšia veľmi krátka papilárna línia. Prípad m7 je tvorený samostatnou krátkou papilárnou líniov. Markanty sú odstránené, ak splňujú jednu z týchto podmienok:

1. Ak je vzdialenosť medzi jednou vidlicou a ukončením menšia ako nastavený prah a dva markanty sú na jednej papilarnej líniov, odstránia sa oba markanty, ukončenie aj vidlica.
2. Ak je vzdialenosť medzi dvoma vidlicami menšia ako nastavený prah a nachádzajú sa na rovnakej papilarnej líniov, sú odstránené. To platí pre prípad m2 a m3.
3. Ak sú dve ukončenia vo vzdialenosti, ktorá je blízka prahovej hodnote a majú podobný smer.

4. Ak vyhovujú podmienke, že nie je žiadne ďalšie vetvenie medzi týmito ukončeniami, sú považované za falošné markanty a sú automaticky odstránené. Tato situácia platí pre prípady m4, m5, m6.
5. Ak sú dve ukončenia umiestnené na krátkej papilárnej línii a vzdialenosť je menšia ako nastavený prah.

Výhodou tohto postupu navrhnutom v [12] je, že tretí krok odstráni markanty typu m3, m4, m5 v jednej procedúre a taktiež sa tým zníži výskyt markantov typu m7.

Výpočet orientácii markantov

Keďže rôzna kvalita, podmienky a tlak môžu ľahko zmeniť typ markantu, väčšina vedeckých pracovníkov prijala jednotnú metodiku vyjadrenia markantov, ktorá v sebe zahrnuje oba typy markantov ukončenie a rozdvojenie. Každý markant je teda jednoznačne charakterizovaný parametrami: súradnica v osi x, súradnica v osi y, a orientáciou.

Výpočet orientácie markantu typu ukončenie je založený na prechádzaní papilárnej línie od pozície markantu $[t_x, t_y]$ ďalej po papilárnej línii až k bodu $[l_x, l_y]$ konečným počtom krokov D. Následne je vypočítaná orientácia markantu pomocou vzťahu

$$\theta = \text{atan} \frac{s_y - t_y}{s_x - t_x}$$

Výpočet orientácie vidlice spočíva v rozdelení vidlice do troch samostatných ukončení a orientácia každého z nich je vypočítaná ako vo vyššie uvedenom vzťahu. Výsledkom sú tri hodnoty orientácii. Následne sú vypočítané hodnoty rozdielov medzi týmito uhlami. Uhol, ktorého veľkosť rozdielu od ostatných dvoch uhlov je najväčšia je určený ako skutočný uhol orientácie markanty.[12]

7 Porovnávanie odtlačkov prstov

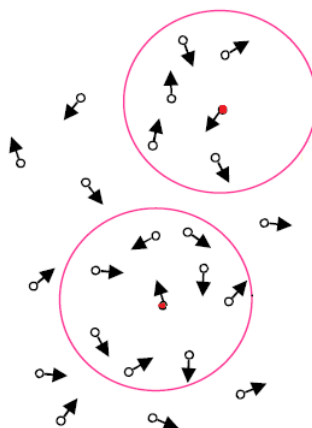
Tato časť práce popisuje algoritmus popísaný Chenom, Sumom a Lamom v článku[16].

Spôľahlivosť a rýchle porovnávanie odtlačkov prstov je stále náročný problém. Autori navrhli algoritmus, ktorý používa centrovane kruhové oblasti okolo jednotlivých markantov, ktoré zabezpečujú odolnosť voči nelineárnemu skresleniu a potrebnú rýchlosť. Kruhová oblasť je vytvorená okolo každého markanty. Oblasť vytvorená okolo každého markanty tvorí len malú časť odtlačku a to zabezpečuje väčšiu tolerantnosť voči nelineárnym skresleniam oproti technikám porovnávajúcim markanty v globálnom tvare.

Popisovaný algoritmus vychádza z extrahovaných markantov, ktoré sú určené svojou pozíciou a orientáciou. Algoritmus je možné rozdeliť do troch častí:

1. V prvom kroku sú vytvorené kruhové regióny okolo každého markantu
2. Sú porovnávané regionálne oblasti odtlačkov pokiaľ nie je nájdená prvá zhoda dvoch regiónov.
3. Keďže je kruhový región definovaný markantami v jeho strede a je možné nájsť viacero párov markantov [16]

Nech $\{A_0, A_2, A_3 \dots A_N\}$, predstavujú množinu markantov v odtlačku a $K(A_i)$ je kruhový región s markantom A_i v jeho strede (Obrázok 7.1). Každý vytvorený región je reprezentovaný stredovým markantom a množinou markantov v jeho bezprostrednom okolí.



Obrázok 7.1 Kruhové regióny vytvorené okolo markantov.[16]

Nech $\{A_0, A_2, A_3 \dots A_{M-1}\}$ je množina markantov v porovnavej šablóne a $\{B_0, B_1, B_2, B_3 \dots B_{K-1}\}$ je množina markantov v zosnímanom odtlačku. $\{K(A_0), K(A_1), \dots, K(A_{m-1})\}$ predstavuje množinu kruhových regiónov v uloženej šablóne a $\{K(B_0), K(B_1), \dots, K(B_{m-1})\}$ je množina regiónov porovnávaného odtlačku.

Algoritmus porovnáva kruhový región $K(A_i)$ s regiónom $K(B_j)$. Centrálné markanty v kruhových regiónoch sú označené ako rovnaké ak zhoda dosiahnutá v najbližšom okolí dosiahla minimálny prah.

Markanty A_i a B_j budeme uvažovať ako referenčné markanty. Nech A je markant v $\{K(A_i)\}$ a B markant v $\{K(B_j)\}$. Proces, ktorý rozhoduje, či sú markanty A a B označené ako rovnaké je možné popísať nasledovne.

$A(x(A), y(A), \alpha(A))$ je markant regiónu $K(A_i)$ a $B(x(B), y(B), \alpha(B))$ je markant regiónu $K(B_j)$. Markanty sú konvertované do polárneho súradnicového systému s ohľadom na príslušný referenčný markant. Nech $A(r(A), \theta(A), \beta(A))$ a $B(r(B), \theta(B), \beta(B))$ predstavujú markanty A a B v systéme polárnych súradníc, kde r je veľkosť vzdialenosti od začiatku sústavy súradníc, θ je uhol ktorý zvierá r s horizontálnou osou. β je uhol orientácie markantu (s prihliadnutím k referenčnému markantu).

Markanty A a B sú označené ako rovnaké ak sú splnené všetky tieto podmienky:

$$\left\{ \begin{array}{l} |r(A) - r(B)| < \text{prah}(r) \\ |\theta(A) - \theta(B)| < \text{prah}(\theta) \\ |\beta(A) - \beta(B)| < \text{prah}(\beta) \\ \sqrt{(r(A) - r(B))^2 + (\theta(A) - \theta(B))^2 + (\beta(A) - \beta(B))^2} < \text{prah}(T), \end{array} \right.$$

Prahové hodnoty určujú maximálnu povolenú toleranciu zmeny r, θ, β .

Vstupné hodnoty do porovnávacej funkcie, sú definované nasledovne:

zavedieme premennú: $Da = \alpha(B_j) - \alpha(A_i)$, potom

$$r(A) = \sqrt{[x(A) - x(A_i)]^2 + [y(A) - y(A_i)]^2}$$

$$\theta(A) = \left\{ \begin{array}{l} 90; x(A) = x(A_i), y(A) > y(A_i) \\ -90; x(A) = x(A_i), y(A) < y(A_i) \\ 0; x(A) = x(A_i), y(A) = y(A_i) \\ \left(\text{atan} \frac{y(A) - y(A_i)}{x(A) - x(A_i)} \right) \times \frac{180}{\pi} + 180; x(A) < x(A_i) \\ \left(\text{atan} \frac{y(A) - y(A_i)}{x(A) - x(A_i)} \right) \times \frac{180}{\pi}; x(A) > x(A_i), y(A) \geq y(A_i) \\ \left(\text{atan} \frac{y(A) - y(A_i)}{x(A) - x(A_i)} \right) \times \frac{180}{\pi} + 360; x(A) > x(A_i), y(A) < y(A_i) \end{array} \right.$$

$$\beta(A) = \alpha(A)$$

Po prepočítaní do polárnych súradníc sa pokračuje regiónom B. Jednotlivé parametre sú vypočítané s prihliadnutím na región A.

$$r(B) = \sqrt{[x(B) - x(A)]^2 + [y(B) - y(A)]^2}$$

Zavedieme premennú:

$$temp = \begin{cases} 90; x(A) = x(A_i), y(A) > y(A_i) \\ -90; x(A) = x(A_i), y(A) < y(A_i) \\ 0; x(A) = x(A_i), y(A) = y(A_i) \\ \left(atan \frac{y(A) - y(A_i)}{x(A) - x(A_i)} \right) \times \frac{180}{\pi} + 180; x(A) < x(A_i) \\ \left(atan \frac{y(A) - y(A_i)}{x(A) - x(A_i)} \right) \times \frac{180}{\pi}; x(A) > x(A_i), y(A) \geq y(A_i) \\ \left(atan \frac{y(A) - y(A_i)}{x(A) - x(A_i)} \right) \times \frac{180}{\pi} + 360; x(A) > x(A_i), y(A) < y(A_i) \end{cases}$$

$$temp = temp - Da; potom$$

$$\theta(B) = \begin{cases} temp - 360; temp \geq 360 \\ temp - 360; temp < 0 \\ temp; 0 \leq temp \leq 360 \end{cases}$$

$$\beta(B) = \begin{cases} \alpha(B) - Da; \alpha(B) - Da \geq 0 \\ \alpha(B) - Da + 360; \alpha(B) - Da < 0. \end{cases}$$

Ak je v dvoch porovnávaných regiónoch nájdený dostatočný počet zhodných okolitých markantov sú tieto regióny považované za zhodné. Tato operácia sa opakuje pre všetky regióny v odtlačkoch pokiaľ nie je získaný celkový počet zhodných markantov. Následne je vypočítané skóre

$$skóre = \frac{pocet_zhodných_markantov}{(pocet_markantov_v_odtlackuA + pocet_markantov_v_odtlackuB)/2} \times 100\%$$

, ktoré určuje percentuálnu podobnosť dvoch odtlačkov v rozsahu 0-100%. Ak je výsledné skóre vyššie alebo rovné stanovenému prahu je vykonaná určitá akcia, podľa určenia a funkcie biometrického systému (povolenie vstupu, autentizácia ...).

8 Právna problematika využitia biometrických údajov

V tejto kapitole som čerpal z týchto zdrojov [17], [18] , [19].

Rozoberiem právne problémy súvisiace so spracovaním biometrických údajov v Českej republike podľa platných zákonov a legislatívy.

Ochranu osobných údajov rieši na najvyššej úrovni Ústava České republiky. Podľa § 3 zákona č. 1/1993 Sb., Ústava České republiky, v platnom znení je súčasťou ústavného poriadku Českej republiky aj Listina základných práv a slobôd. V článku 10., odstavce 3 sa hovorí, citujem: „Každý má právo na ochranu pred neoprávneným shromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe.“

Aby nebol porušovaný tento článok bol zákonom č 101/2000 Sb. zriadený „Úrad pro ochranu osobních údajů se sídlem v Praze“.

Úrad pro ochranu osobních údajů (ÚOOÚ) je nezávislý orgán, ktorý dozerá na dodržiavanie zákonom stanovených povinností pri spracovaní osobných údajov, vedie register povolených spracovaní osobných údajov, prijíma podnety a sťažnosti občanov na porušovanie zákona a poskytuje konzultácie v oblasti ochrany osobných údajov.

Zmyslom zákona o ochrane osobných údajov je zaručené právo na ochranu občana pred neoprávneným zasahovaním do jeho súkromného a osobného života neoprávneným zhromažďovaním a zverejňovaním alebo iným zneužívaním osobných údajov. Z vecného hľadiska sa zákon vzťahuje na všetky osobné údaje ,teda nie len na tie, ktoré sú vedené automatizovane v informačných systémoch. Z hľadiska osobnej pôsobnosti sa zákon vzťahuje na všetkých právne subjekty(fyzické i právnické osoby).

V zákone 101/2000 Sb., § 4 je stanovené, čo je osobný alebo citlivý údaj, citujem:

„ a) osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímou identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu,

b) citlivým údajem osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj

subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů“.

Odtlačok prsta je biometricky údaj a preto je považovaný za citlivý údaj. Pre citlivý údaj platia rovnaké normy ako pre údaj osobný avšak s určitými prísnejšími nariadeniami.

V tomto zákone § 9 je stanovené v akom prípade je možné spracovávať citlivé údaje. Zákon 101/2000 Sb., § 9, citujem : „Citlivé údaje je možno spracovávať len, jestliže:

- a) subjekt údajů dal ke zpracování výslovný souhlas. Souhlas musí být dán písemně, podepsán subjektem údajů a musí z něho být zřejmé, k jakým údajům je dáván, jakému správci údajů, k jakému účelu, na jaké období a kdo jej poskytuje. Souhlas může subjekt údajů kdykoliv odvolat. Správce je povinen předem subjekt údajů o jeho právech poučit. Tento souhlas musí správce uschovat po dobu zpracování osobních údajů, k jejichž zpracování byl souhlas dán
- b) je to nezbytné v zájmu zachování života nebo zdraví subjektu údajů nebo jiné osoby nebo odvrácení bezprostředního závažného nebezpečí hrozícího jejich majetku, pokud není možno jeho souhlas získat zejména z důvodů fyzické, duševní či právní nezpůsobilosti, v případě, že je nezvěstný nebo z jiných podobných důvodů. Správce musí ukončit zpracování údajů, jakmile pominou uvedené důvody, a údaje musí zlikvidovat, ledaže by subjekt údajů dal k dalšímu zpracování souhlas,“.

Zákon jasne hovorí o tom, kedy a akým spôsobom je možné požadovať citlivý údaj, §9 písm.b) je chápaný ako celkom výnimočný prípad.

Ďalej sú v zákone 101/2000 Sb., § 13 definované povinnosti osôb pri zabezpečení osobných údajov, citujem: „Správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů“.

Týmto ustanovením sú stanovené všeobecné povinnosti pre všetkých správcov, tykajúce sa zaistenia ochrany osobných údajov a ich bezpečnosti. Ošetreniami ktoré má správca podniknúť sa rozumejú technické, organizačné a právne opatrenia. Údaje musia byť chránené voči zamestnancom, tak iným osobám, ktoré s nimi prichádzajú oprávnene do styku tak napr. voči akýmkoľvek iným osobám. Konkrétne opatrenia sú závislé na rozsahu a použití prostriedkov, ktoré správca pri spracovaní použije.

Zákon 101/2000 Sb., § 4 taktiež stanovuje pojmy uchovávanie osobných údajov, blokovanie osobných údajov a likvidácia osobných údajov, citujem:

„g) uchovávaním osobních údajů udržování údajů v takové podobě, která je umožňuje dále zpracovávat,

h) blokováním osobních údajů vytvoření takového stavu, při kterém je osobní údaj určitou dobu nepřístupný a nelze jej jinak zpracovávat,

i) likvidací osobních údajů se rozumí fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalších zpracování, “.

Za likvidáciu nie je považovaný taký spôsob, po ktorého aplikácii by bolo možné inými technickými prostriedkami tieto údaje obnoviť ,aby mali charakter osobných údajov.

Zákon 101/2000 Sb., § 4 taktiež definuje pojmy správca a spracovateľ osobných údajov, citujem:

„j)správcom každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak,

k)zpracovatelem každý subjekt, který na základě zvláštního zákona nebo pověření správcom zpracovává osobní údaje podle tohoto zákona“.

Správcom s rozumie aj fyzická osoba , ktorá spracováva osobné údaje pre účely podnikateľské alebo akékoľvek iné účely. Pokiaľ ide o súkromné subjekty, môže osobné údaje spracovávať, len pokiaľ to zákon nezakazuje .Správca môže poveriť, aby osobné údaje spracovával iný subjekt, tj. spracovateľ.

Zákon taktiež stanovuje povinnosti správcu. Zákon 101/2000 Sb., § 5 ods. (1), citujem:

„Správce je povinen: a) stanovit účel, k němuž mají být osobní údaje zpracovány, b) stanovit prostředky a způsob zpracování osobních údajů “. Uvedené povinnosti musí správca plniť dopredu a náležite o nich informovať dotknute osoby.

Spracúvať biometrické údaje možno len ak to prevádzkovateľovi vyplýva výslovne zo zákona, alebo na spracovanie dala písomný súhlas dotknutá osoba. Výnimkou je, ak sa biometrické údaje spracúvajú na účely evidencie alebo identifikácie vstupu do citlivých, osobitne chránených objektov, vyhradených priestorov alebo prístupu do technických zariadení alebo prístrojov s vysokou mierou rizika

Ak majú byť spracované študentove citlivé osobne údaje vyplniťformular, ktorý je uvedený na nasledujúcej strane:

Souhlas osoby se zpracováním osobních a citlivých údajů

Jméno a příjmení

Správce osobních údajů (zpracovatel): Vysoká škola báňská – Technická univerzita Ostrava, IČ: 61989100, sídlem Ostrava, 17. listopadu 15, PSČ 708 33.

Souhlasím, dle ustanovení zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, se zpracováním mých osobních a citlivých údajů *zpracovatelem* , kterými jsou:

- otisky prstů,
- jméno a kontakt na kontaktní osobu ,
- jméno a příjmení ,

po dobu od
 do

Podpis

9 Implementácia v systéme eLogika

Systém eLogika je elektronický informačný systém na katedre informatiky FEI VŠB-TU. Umožňuje študentovi absolvovať písomnú časť skúšky formou on-line testu. Implementované využitie biometrického overenia totožnosti študenta počíta s dvoma scenármi. Študenti dištančnej formy štúdia nemusia byť vždy schopný sa v určený čas dostaviť na absolvovanie skúšky z absolvovaného predmetu. V takom prípade môžu absolvovať skúšku z pohodlia domova, avšak pod podmienkou overenia ich totožnosti pomocou odtlačku prstu, pre vylúčenie možnosti podvodu.

Druhý scenár sa týka absolvovania skúšky písomnou formou. Súčasný stav je taký, že študent preukazuje svoju totožnosť pomocou študentskej karty (ISIC). V minulosti bolo však zaznamenaných množstvo pokusov o podvod (iný študent na skúške, zmena fotky atd.). Preto študent poskytne pre overenie svojej totožnosti odtlačok prsta.

Podľa zákona o ochrane osobných údajov je možné spracovávať biometrický údaj len ak to vyplýva zo zákona alebo so súhlasom dotknutej osoby. V našom prípade je potrebný súhlas študenta. Správca údajov musí presne stanoviť na aký účel budú tieto údaje určené, kto a v akom rozsahu bude s nimi pracovať a uchovávať tieto údaje len po vymedzené a oboma stranami známe časové obdobie a náležite tieto údaje zabezpečiť. Zákon o ochrane osobných údajov bližšie neurčuje, aké kroky má správca údajov pre zabezpečenie podniknúť.

V praktickej časti diplomovej práce bola implementovaná metóda vylepšenia vstupného obrazu pomocou gáborových filtrov. Následne detekcia markantov a algoritmus pre porovnávanie odtlačkov popísaný v teoretickej časti. Aplikácia bola vytvorená v prostredí Microsoft Visual Studio 2010, na platforme .Net 4.0 v jazyku C# a bola prepojená so systémom eLogika

Aplikácia je rozdelená na tieto časti:

- **Klient**
- **Server**

9.1 Klient

V praktickej realizácii boli vytvorené dve aplikácie. Prvá je určená pre pridávanie šablón odtlačkov do systému a druhá umožňuje overenie identity pri vykonávaní obline testu v systéme eLogika.

Aplikácia umožňuje pridávanie odtlačkov, ich správu, verifikáciu a identifikáciu študenta vo zvolenej množine študentov. Druhá aplikácia umožňuje absolvovať skúšku cez webové rozhranie z domova. Po otvorení a zadaní svojich prihlasovacích údajov do systému eLogika je overená jeho totožnosť, následne je študent verifikovaný odtlačkom prsta a v úspešnom prípade je mu umožnené absolvovať vybranú úlohu cez webové rozhranie systému eLogika.

K využívaniu týchto aplikácií je nutné vlastniť funkčný užívateľský účet v systéme eLogika[20], mať potrebné užívateľské práva a čítačku prstov Futronic FS 88 pre získavanie odtlačkov prstov a ich overovanie.

Klientské aplikácie zabezpečujú priespracovanie a vylepšenie obrazu odtlačku a extrakciu špecifických znakov nutných pre porovnávanie. Ich verifikácia alebo identifikácia prebieha až na serveri. Klient komunikuje so serverom zabezpečenými webovými službami.

Jednotlivé prípady využitia týchto aplikácií sú popísané v prílohe

Aplikácie sú umiestnené v prílohe.

9.2 Server

Na serveri sú implementované metódy pre identifikáciu a verifikáciu odtlačku. Server zabezpečuje komunikáciu s databázou a poskytuje webové služby pomocou ktorých môže klientska aplikácia komunikovať. Pre vzájomnú komunikáciu boli využité implementované služby systému, ktoré sú popísané v [21] a boli doplnené o potrebné špecifické funkcie ako je porovnávanie šablón odtlačkov prstov, ich ukladanie do databázy, verifikácia a identifikácia študentov, .

Snímacie zariadenie:

Pre samotné snímanie odtlačkov prstov je použitá čítačka Futronic Fs88. Je to dotykový snímač so SMOS senzorom, s rýchlosťou snímania odtlačku do 100ms, výstupom je 8.bitový šedo tónový obraz a je pripojená pomocou USB portu. Rozlíšenie získaného obrazu je 480x320 pixlov pri 500 dpi.(Obrázok 9.1)[20]



Obrázok 9.1 Futronic FS 88.

9.3 Realizácia vylepšenia obrazu a detekcie markantov:

Na obrázku (Obrázok 9.2) je zobrazený zosnímaný obraz z čítačky odtlačkov prstov Futronic FS 88. Jedná to o 8 bitový obraz v rozlíšení 480 X 360 pixelov.



Obrázok 9.2 Zosnímaný obraz.

Výpočet orientovaného obrazu je realizovaný podľa postupu v kapitole Výpočet orientácií papilárnych línií. Orientácie sú vypočítané samostatne pre každý pixel, čo umožňuje presnejšiu aplikáciu Gaborových filtrov. Orientovaný obraz je použitý aj pri výpočte frekvencií hrebeňov papilárnych línií, avšak tu sú jednotlivé orientácie vypočítané na bloky 32×32 pixelov. Pre lepšiu názornosť sú v obrázku (obrázok) znázornené orientácie blokov 16×16 pixelov (Obrázok 9.3)..



**Obrázok 9.3 Zobrazenie vypočítaných orientácií hrebeňov papilárnych línií,
v blokoch 16 x 16 px.**

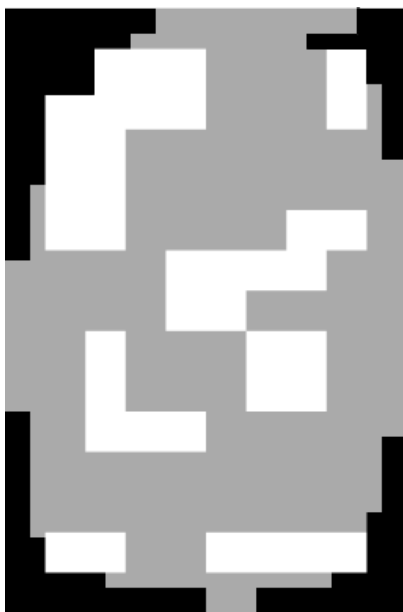
Výpočet normalizovaného obrazu a segmentácie je popísaný v kapitolách Normalizácia a Segmentácia. Čierne bloky v obraze znázorňujú miesta v obraze s nízkou hodnotou variácie pixelov. Medzný prah, ktorý určuje, či bude blok určený do pozadia, bol nastavený tak, aby neboli za pozadie považované oblasti odtlačku zosnímané pod nedostatočným tlakom ale len skutočné okolie odtlačku. Normalizácia upravuje hodnoty pixelov do požadovaného rozsahu pre spracovanie v ďalších častiach úpravy Gaborovými filtermi. Samotná normalizácia nemení priebeh papilárnych línií, ale pre zvýraznenie papilárnych línií som použil rozťahnutie kontrastu.



Obrázok 9.4 Spojený normalizovaný obraz s vyznačenými blokmi pozadia obrazu.

Na obrázku (Obrázok 9.5) je znázornená vypočítaná frekvencia hrebeňov papilárnych línií v blokoch 32×32 pixelov. Táto veľkosť bloku sa pre výpočet frekvencií hrebeňov ukázala ako najlepšia. Bloky, ktorých orientácia sa nedá vypočítať (bloky s vysokým šumom, bloky s výskytom markantov)

sú doplnené priemernou hodnotou z blokov v najbližšom okolí. Bloky, ktorých najbližšie okolie nemá pri tomto procese vypočítanú frekvenciu sú doplnené priemernou hodnotou vypočítaných frekvencií. Na obrázku sú znázornené frekvencie po vyhladení Gaussovým filtrom a sú im priradené hodnoty, podľa toho ktorej hodnote frekvencie banky Gaborových filtrov ($1/6$, $1/9$, $1/12.5$) sa najviac blížia. V extrémnom prípade môže nastať situácia, že sa nepodari vypočítať frekvenciu ani pre jeden blok, v tomto prípade sú nastavené hodnoty frekvencií všetkých blokov na hodnotu $1/9$, samozrejme s výnimkou pozadia obrazu.



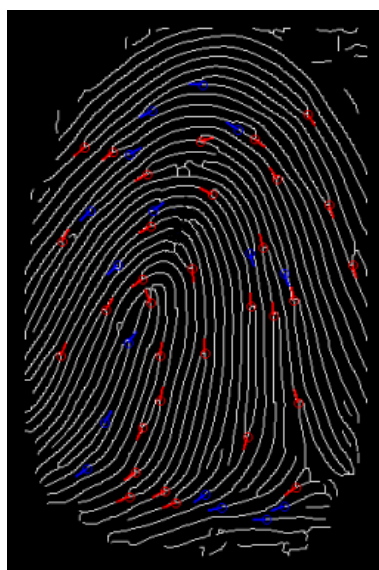
Obrázok 9.5 Frekvenčný obraz.

Na obrázku (Obrázok 9.6) je znázornený obraz, ktorý je výsledkom Gaborovej filtrácie a bolo na ňom vykonané jednoduché prahovanie (prah má hodnotu 0, body s vyššou hodnotou sú považované za hrebene papilárnych línií, body s hodnotou rovnou 0 a nižšou sú považované za údolia papilárnych línií alebo za pozadie obrazu). V [1] sú použité hodnoty frekvencií pre vytvorenie banky Gaborových filtrov $1/5$, $1/7$, $1/9$. Thai vo svojom publikovanom článku [11] neuvádza, aké hodnoty frekvencií používa. V mojej implementácii som použil hodnoty frekvencií $1/6$, $1/9$, $1/12.5$, ktoré zohľadňujú fakt, že hustota hrebeňov papilárnych línií je u ľudí veľmi variabilná. Banka Gaborových filtrov je vypočítaná pre orientácie s krokom 22.5 stupňa, hodnota orientácie každého bodu je zaokrúhlená a je jej priradená jedna z hodnôt 1-8 (22.5° - 180°) tak ako je uvedené v [1]. Je vytvorená banka, ktorá obsahuje 24 filtrov (3 frekvencie x 8 orientácií). V [1] je odporúčaný parameter odchýlok pre jednotlivé filtre $\sigma_x = \sigma_y = 4$, Thai uvádza ako najlepší kompromis hodnotu 2, experimentálne sa ako najlepšia ukázala hodnota z [1], hrebene papilárnych línií po vyhladení majú lepší priebeh a je nájdených menej falošných markantov.



Obrázok 9.6 Binárny obraz.

Na binárny obraz je aplikovaný tenčiaci algoritmus popísaný v kapitole Skeletizácia binárneho obrazu. Po získaní kostry sú vyhľadané markanty. Na okrajoch odtlačku je nájdené veľké množstvo falošných ukončení. Tieto markanty sú ihneď odstránené, pretože sa nachádzajú veľmi blízko blokov, ktoré tvoria segmentovaný obraz pozadia. Pre toto odstránenie som použil metódu knižnice Emgu[22] *findcontures*, ktorá vráti obrys pozadia obrazu. Body, ktoré sa nachádzajú vo vzdialenosti do 15 pixelov od obrysu pozadia nebudú považované za markanty. Funkcia *findcontures* je použitá aj na hrebene papilárnych línií, aby bolo možné rozlíšiť, či sa markanty nachádzajú na rovnakej papilarnej línií. Následne sú odstránené ďalšie falošné markanty postupom popísaným v kapitole Odfiltrovanie falošných markantov. Pre markanty, ktoré prešli filtráciou je vypočítaná orientácia podľa postupu v teoretickej časti v kapitole Výpočet orientácii markantov.



Obrázok 9.7 Kostra obrazu s nájdenými markantami typu rozdvojenie a ukočenie

9.4 Výsledky

Použité prahové hodnoty pre porovnávanie odtlačkov sú:

$$prah(r)=10$$

$$prah(\theta)=12$$

$$prah(\beta)=12$$

$$prah(T)=30$$

Tieto použité hodnoty sa pri testovaní preukázali najlepšie. Dostačme zohľadňujú elasticnosť prsta a odchýlky spôsobené rôznym tlakom a orientáciou priloženia prstu . V prípade, že je pri identifikácii nájdených viacero užívateľov u ktorých je vypočítaná zhoda prekonávajúci prekonávajúca percentuálny prah, vyberie sa užívateľ s najvyšším skóre.

Pre hodnotenie výkonnosti biometrických systémov sú používané hodnotiace indexy výkonnosti FRR (pravdepodobnosť chybného odmietnutia) a FAR (pravdepodobnosť chybného odmietnutia) popisované v kapitole Výkonnosť biometrických systémov. Pre hodnotenie výkonnosti bola použitá databáza obsahujúca 40 odtlačkov (jeden prst bol v sade obsiahnutý 4 krát) .Sadá odtlačkov bola získaná snímacím zariadením Futronic FS 88.

Najprv boli experimentálne získané rozdelenia miery zhody odtlačkov oprávnených osôb (odtlačky rovnakých prstov) a odtlačkov neoprávnených osôb (odtlačky rôznych prstov). V rozdelení neoprávnených osôb bolo najviac odtlačkov sústredených okolo hodnoty skóre 10 %. Zatiaľ, čo rozdelenie zhody oprávnených osôb je viac rozťahnuté a najviac rovnakých odtlačkov má zhodu okolo 35 %. Prienikom týchto hodnot bolo zistené EER 13% pri veľkosti skóre 25%. Medzný prah bol zvolený 40%

Pomocou hodnôt z grafu boli vypočítané veľkosti chýb FAR A FRR

Záver

V tejto práci boli zhrnuté poznatky o odtlačku prsta a ponúkol som určitý náhľad do ostatných biometrických metód. Problematika automatizovaného spracovania odtlačkov prstov je veľmi rozsiahla a venuje sa jej veľké množstvo odborných článkov. Teoretická časť práce je zameraná na popis jednotlivých krokov spracovania odtlačkov a uvádza vybrané metódy, ktoré sú pri týchto krokoch využité a implementované.

Z množiny použiteľných biologických charakteristík pre identifikáciu sa odtlačok prsta javí ako jeden z najprijateľnejších, hlavne pre svoju prirodzenosť. Teoreticky som popísal metódu a následne implementoval metódu vylepšenia zosnímaného obrazu odtlačku Gáborovou filtráciou. Ako výhoda tejto filtrácie sa preukázal fakt, že je vytvorená sada filtrov zohľadňuje smer i frekvenciu hrebeňov papilárnych línií a dostatočná odolnosť voči šumu.

Porovnávajúci algoritmus sa preukázal ako dostatočne robustný, aj keď vykazuje veľké množstvo falošných odmietnutí. Pri nižšom prahu má síce väčšiu priepustnosť ale taktiež vzniká šanca prepustenia neoprávnenej osoby.

Možným rozšírením tejto práce by mohlo byť dôkladné rozobratie metód pre klasifikáciu odtlačkov a implementácia funkcie, ktorá by dokázala zaradiť odtlačok do kategórie podľa klasifikačnej schémy. Za ďalšie štúdium určite stojí literatúra, popisujúca pokročilé metódy porovnávania prstov.

Použitá literatura

- [1] **MALTONI, Davide, Darion MAIO, Anil K. JAIN a Salil PRABHAKAR.** *Handbook of finger print recognition*. New York: Springer-Veglag, 2003, 341 s. ISBN 0-387-95431-7.
- [2] **ŠČUREK, Radomír.** VŠB TU OSTRAVA, Fakulta bezpečnostního inženýrství. *Biometrické metody identifikace osob v bezpečnostní praxi: Studijní text*. 2008. Dostupné z: www.fbi.vsb.cz/miranda2/export/sites-root/fbi/040/cs/sys/resource/PDF/biometricke_metody.pdf
- [3] **VACH, Martin.** *Historie biometrik a jejich využití ve výpočetní technice* [online]. [cit. 2012-04-15]. Dostupné z: http://www.fi.muni.cz/usr/jkucera/pv109/2003/xvach_biometriky.htm
- [4] **RAK, Roman, Matyáš VÁCLAV a Říha ZDENĚK.** *Biometrie a identita člověka: ve forenzních a komerčních aplikacích*. Brno: Grada Publishing, 2008, 664 s. ISBN 978-80- 247-2365-5.
- [5] **WAYMAN, James L.** Error-Rate Equations for the General Biometric System: Enhancing human-identification systems through multiple samples, multiple templates and database-partitioning techniques. 1999, s. 35-48. Dostupné z: <http://ai.pku.edu.cn/aiwebsite/research.files/collected%20papers%20-%20performance%20evaluation/Error%20rate%20equations%20for%20the%20general%20biometric%20system.pdf>
- [6] **COUFAL, Tomáš.** Co je to FingerChip. [online]. [cit. 2012-03-15]. Dostupné z: <http://www.hw.cz/teorie-a-praxe/co-je-to-fingerchipr.html>
- [7] Optoelektronické snímače otisků prstů. [online]. [cit. 2012-05-02]. Dostupné z: http://www.zld.cz/cinnost/vyvoj/biometrie/sni_opt.php?p=2|6|8|26|
- [8] **WEI, Liu.** Fingerprint Classification Using Singularities Detection. 2008. Dostupné z: <http://www.naun.org/journals/mcs/mcs-87.pdf>
- [9] **KOVÁČ, Petr.** *Návrh biometrického identifikačního systému pro malou organizaci*. Zlín, 2009. 85 s. Diplomová práce.
- [10] BIOIDENTIFICATION: Frequently Asked Questions. [online]. [cit. 2012-05-02]. Dostupné z: <http://www.bromba.com/faq/fpfaq.htm#Fingerprint-Sensoren>
- [11] **THAI, Raymond.** *Fingerprint Image Enhancement and Minutiae Extraction*. 2003. Dostupné z: <http://www.csse.uwa.edu.au/~pk/studentprojects/raymondthai/RaymondThai.pdf>
- [12] **ZHILI, Wu.** *Fingerprint Recognition* [online]. 2002 [cit. 2012-05-02]. Dostupné z: <http://www.comp.hkbu.edu.hk/~vincent/hp/fingerprintRecognition.doc>
- [13] **ŠMÍD, Vladimír.** Srovnání právních úprav vztahujících se k ochraně osobních údajů v ČR a SR. [online]. [cit. 2012-05-02]. Dostupné z: <http://www.fi.muni.cz/~smid/ochdcrsr1.html>

- [14] **HONG, Lin, Yiefei WAN a Anil JAIN.** Fingerprint Image Enhancement: Algorithm and Performance Evaluation. 1998, s. 777-789. Dostupné z: <http://www.cse.msu.edu/biometrics/Publications/Fingerprint/MSU-CPS-97-35fenhance.pdf>
- [15] **DOBEŠ, Michal.** *Zpracování obrazu: a algoritmy v c#*. 1. vydání. Praha: BEN, 2008. ISBN 978-80-7300-233-6.
- [16] **CHEN, Haiyong, Hongwei SUN a Kwok-Yan LAM.** A fast and elastic fingerprint matching algorithm using minutiae-centered circular regions. *A fast and elastic fingerprint matching algorithm using minutiae-centered circular regions*. 2007, s. 211-215. Dostupné z: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4385335&tag=1>
- [17] Úrad pro ochranu osobních údajů, Zákon č. 101/2000 Sb., o ochraně osobních údajů, [online], aktualizované: 1.1.2012, [cit. 2012-01-01], Dostupné z: <http://www.uouu.cz/uouu.aspx?menu=4&submenu=5&loc=20>
- [18] Ústava České republiky. [online]. [cit. 2012-05-02]. Dostupné z: <http://www.psp.cz/docs/laws/constitution.html>
- [19] **LEPEŠKA, Stanislav.** *VYUŽITÍ BIOMETRICKÝCH ÚDAJU VE STÁTNÍ SPRÁVĚ*. 2008. Dostupné z: <https://dspace.vsb.cz/bitstream/handle/10084/69660/B6202.6202R009.lep014.pdf?sequence=1>
- [20] Futronic FS88 FIPS201/PIV Compliant USB2.0 Fingerprint Scanner. Dostupné z: http://www.futronic-tech.com/download/FS88_brochure.pdf
- [21] **HERNAS, Vojtěch.** *Systém eLogika a e-learningová podpora výuky*. Dostupné z: https://dspace.vsb.cz/bitstream/handle/10084/89513/HER171_FEI_N2647_2612T025_2011.pdf?sequence=1. Diplomová práce. Vysoká škola báňská-TU Ostrava.
- [22] [online]. [cit. 2012-05-02]. Dostupné z: http://www.emgu.com/wiki/index.php/Main_Page